Name _____

Exam 2 – CSIS 3755

True/False
Indicate whether the statement is true or false.

____ 1. A port is a network sub-address (assigned a number between 0 and 65,535) through which a particular type of data is allowed to pass.

____ 2. Distributed denial-of-service (DDoS) attacks occur when an attacker floods a server with requests coming from many different sources under their control.

____ 3. A firewall centralizes security for the organization it protects.

____ 4. A firewall is an ideal endpoint for a VPN.

____ 5. Packet filtering is a key function of any firewall.

____ 6. Additional segmented sections at the end of a packet are called either a footer or a tailer.

____ 7. Stateless packet filtering is of no value at all.

____ 8. A stateful packet filter has the ability to maintain a record of the state of a connection.

____ 9. The most important benefit of using a proxy server is for redirecting URLs.

____ 10. Proxy servers can be configured to strip out Java applets if you don't want them to enter the network.

____ 11. One way to configure your firewall is by setting rules.

____ 12. Scalability is definitely a concern if you use a proxy server.

____ 13. The Principle of Least Priviledge first restricts all transmissions except a specific set of services.

____ 14. Neither a demilitarized zone (DMZ) nor a service network need IP addresses.

____ 15. A firewall inspects packets of information when they reach the network perimeter, and, depending on the content of the packet and the firewall rules, sends the packet to the appropriate location or drops it.

____ 16. Encryption is a process that turns information that is plainly readable (plaintext) into scrambled form (ciphertext) in order to preserve the authenticity, integrity, and privacy of the information that passes through the security perimeter.

____ 17. In encryption the most commonly used algorithms include five functions.

____ 18. Encryption is accomplished by using algorithms to manipulate the plaintext into the ciphertext for transmission.

Name _____

____ 19. A digital certificate is similar to a digital signature and asserts that a public key is associated with a particular identity.

____ 20. IP Security (IPSec) is the least dominant cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group.

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

____ 21. Trojan horses enter the system through hidden openings called ____.
a. Application ports
b. Back doors
c. Secret sockets
d. None of the above

____ 22. A ____ connects two companies' networks over the Internet.
a. VPN
b. NAT
c. PAT
d. security

____ 23. At which layer of the OSI model does encryption occur?
a. Application
b. Presentation
c. Session
d. Transport

____ 24. The process of mapping a static public IP address to a private IP address of a computer on the local network is called ____.
a. load balancing
b. IP address mapping
c. content filtering
d. URL filtering

____ 25. Linux has a kernel-level packet filter called ____.
a. TCP/IP filtering
b. IPtables
c. IPsockets
d. Winsock

____ 26. What TCP port is used by Telnet?
a. 80
b. 110
c. 23
d. 72

____ 27. What is a possible cause for an ICMP source quench message?
a. Destination unreachable
b. Faster route located
c. Router receiving too much traffic
d. Too many hops to destination

____ 28. Stateful packet filtering works by controlling the type of transport and the ____ number being used.
a. socket
b. port
c. sequence
d. line

____ 29. FTP uses port ____ for the control port.
a. 20
b. 21
c. 22
d. 23

____ 30. What is the default value of the Internet header length in an IP packet header?
a. 10
b. 15
c. 25
d. 20

Name _____

____ 31. Which of the following is NOT a function of a proxy server?
a. Concealing internal clients
b. Hosting Web sites
c. Blocking URLs
d. Blocking and filtering content

____ 32. When a firewall log is used to determine whether an unauthorized user has accessed resources that should be protected, its function is to ____.
a. uncover weaknesses
b. detect intrusions
c. provide documentation
d. none of the above

____ 33. What is one consideration when choosing a proxy server that must be taken into account as a network grows?
a. Load balancing
b. Scalability
c. Redundancy
d. Fault tolerance

____ 34. In Internet Explorer no proxy server needs to be specified for FTP and Gopher connections because the browser can use the ____ standard.
a. Winsock
b. HTTPS
c. SOCKS
d. CIPS

____ 35. Which of the following types of traffic can be monitored by a proxy server?
a. HTTP
b. DNS
c. SMTP
d. Only a and c
e. a, b, and c

____ 36. What feature of Windows allows you to create multiple proxies that are in use simultaneously?
a. Routing
b. Network Load Balancing
c. Web sharing
d. Clustering

____ 37. Which protocol is typically used to forward all target traffic to the proxy at a single target port?
a. HTTPS
b. Windows sockets
c. SOCKS
d. Name pipes

____ 38. Which of the following proxy applications are open source?
a. T.REX
b. WinGate
c. Squid
d. Both a and c
e. Both a and d

____ 39. Which of the following is ISA Server designed to compete with?
a. FireWall-1
b. Symantec Enterprise Firewall
c. None of the above
d. Both a and b

____ 40. A(n) ____ needs to have sufficient processor speed and memory to handle the network's present traffic and increased traffic as the network grows.
a. bastion host
b. NAT server
c. screening router
d. demilitarized zone

____ 41. Many operating systems perform ____, as do routers.
a. routing
b. packet filtering
c. IP forwarding
d. NAT

Name _____

____ 42. An IDPS system can notify you when ____.
a. the Internet is accessed via a suspicious port
b. a Trojan horse has entered the system
c. someone attempts a TCP port scan
d. all the above

____ 43. If you are a victim of ____, you should consider installing anti-virus software on your SMTP gateway.
a. SYN flooding
b. a virus
c. harmful e-mail messages
d. port scanning

____ 44. When you add a piece of hardware to your network, you need to identify it so your firewall can include it in its ____ services.
a. routing
b. protection
c. both a and b
d. none of the above

____ 45. Rules that permit traffic to your ____ server are essential if your internal users are going to access other computers on the Internet using domain name resolution.
a. DNS
b. NAT
c. Proxy
d. Firewall

____ 46. ____ is when a hacker intercepts part of an encrypted data session to gain control over the data being exchanged.
a. Man-in-the-middle attacks
b. Session hijacks
c. Encryption
d. Public Key

____ 47. ____ is the process of deciphering the original message from an encrypted message, without knowing the algorithms and keys used to perform the encryption.
a. Encryption
b. Cryptography
c. Cryptology
d. Cryptanalysis

____ 48. The mathematical formula or method used to convert an unencrypted message into an encrypted message, or vice versa is a(n) ____.
a. keyspace
b. cipher
c. algorithm
d. work factor

____ 49. The transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components is a(n) ____.
a. cipher
b. algorithm
c. decipher
d. encipher

____ 50. The ____ simply rearranges the values within a block to create the ciphertext.
a. transposition cipher
b. permutation cipher
c. substitution cipher
d. both a and b

Name _____

Yes/No
Indicate whether you agree with the statement.

____ 51. The TTL is a 10-bit value that identifies the maximum time the packet can remain in the system before it is dropped.

____ 52. A stateless packet filter compares the header data against its rule base and forwards only those packets that match a rule.

____ 53. Because ICMP packets have no authentication method to verify the recipient of a packet, hackers can attempt man-in-the-middle attacks, in which they impersonate the intended recipient.

____ 54. Does a stateful filter have a state table that lists current connections?

____ 55. Can a proxy gateway examine the contents of a packet?

____ 56. Are most proxy systems part of a hybrid firewall?

____ 57. Can transparent proxies be configured to be totally invisible to an end user?

____ 58. Is Squid the most popular proxy server for home and small business environments?

____ 59. Does Microsoft ISA Server do more than cache files and provide an application layer proxy gateway?

____ 60. Is application-level gateway another name for a proxy server?

____ 61. Do proxy servers simply insert a new source IP address into the headers of the packets they send out in response to a request?

____ 62. Many companies use the Internet to enable a virtual private network (VPN) that connects internal hosts with specific clients in other organizations.

____ 63. The Cisco CIDS Intrusion Detection System works on external router to notify you of intrusion attempts from the Internet.

____ 64. If you follow a "paranoid" approach to security you will set up application proxy gateways that forward requests on behalf of internal users.

____ 65. The bastion host is the only gateway through which inbound and outbound traffic can pass.

Completion
Complete each statement.

66. A(n) _____ is hardware or software that monitors the transmission of packets of digital information that attempt to pass through the perimeter of a network.

Name _____

67. A _____ is a boundary between two zones of trust.

68. _____ can control the way applications inside the network access external networks by setting up proxy services.

69. A _____ connects two companies' networks over the Internet.

70. What does the authentication process use to protect usernames and passwords? _____

71. The process of mapping a static public IP address to a private IP address of a computer on the local network is called _____.

72. One of the first sets of firewall rules you should establish covers _____, the protocol used to let you test network connectivity.

73. The rules that you set up for _____ need to support two separate connections.

74. The _____ address in the packet header is the address of the computer or device that sent the IP packet.

75. Linux has a kernel-level packet filter called _____.

76. What is the size of the time to live field in an IP packet header? _____

77. What is the maximum length of an IP packet that can be defined in the total length field? _____

78. What tells a firewall how to reassemble a data stream that has been divided into packets? _____

79. A stateless filter compares a packet's header data against its _____ and forwards only those packets that match a rule.

80. What is a possible cause of an ICMP time exceeded message?

81. Proxy servers and packet filters are used together in a _____ but they both inspect different parts of an IP packet.

82. The type of concealment that proxy servers perform resembles _____..

83. A second method of redirecting URLs involves scanning the _____ field in the HTTP packet header.

84. The most common problem in a proxy server is a _____, which occurs when a program attempts to store more data in a temporary storage area than that area can hold.

85. When a firewall log is used to determine whether an unauthorized user has accessed resources that should be protected, its function is to _____.

Name _____

86. _____ is the most common problem a proxy server can fall victim to.

87. A(n) _____ -based approach will have fewer rules because its primary orientation is to let all traffic through and then block specific types of traffic.

88. Your bastion host needs sufficient _____ to support every instance of every program necessary to service the load placed on the machine.

89. A(n) _____ filters and processes requests for URIs and can work in conjunction with firewalls—to call up Web pages from cache if needed.

90. _____ is when a hacker intercepts part of an encrypted data session to gain control over the data being exchanged.

91. Firewall vendors add encryption to their products to provide protection against "active attacks,"which are also known as _____.

92. The transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components is a(n) _____.

93. The information used in conjunction with the algorithm to create the ciphertext from the plaintext is the _____.

94. _____ uses a number of algorithms, but mainly relies on RSA for key transfer and on IDEA, DES, or 3DES for encrypted symmetric key-based data transfer.

95. In a _____, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target.

Short Answer (Type answer on additional pages)

96. In your own words, explain both Caesar cipher and XOR cipher conversion. What is the difference in how these two methods work?

97. Explain the difference between symmetric encryption and asymmetric encryption. What are each methods shortcomings? How can you combine the two methods to overcome each methods shortcoming?

98. What are the three systems use to handle network authentication? Compare two of them.