CYBS 7357 Lab 03 Quiz

\* Answers are highlighted in Yellow

1. Which of the following statements is true regarding firewalls?

a. There are only a few firewalls that are currently available in the commercial marketplace.

b. Firewalls cannot be customized to meet the specific needs of particular organizations.

c. A defense-in-depth structure of firewalls provides more protection for certain subnets than for others.

d. Some organizations establish internal zones to protect the entire organization from outsiders.

2. According to the 2013 Data Breach Investigations Report, \_\_\_\_\_\_\_\_\_\_ percent of all successful data breaches involve internal attackers.

a. one

b. three

c. fourteen

d. thirty-three

3. The job of the \_\_\_\_\_\_\_\_\_\_ is to examine traffic going between the “outside” and the “inside,” determine whether that traffic adheres to a set of rules, and decide what to do if it does not.

a. administrator

b. firewall

c. configuration plan

d. rules planning worksheet

4. Which of the following statements is true regarding firewalls?

a. Firewalls can be completely software based and run on an endpoint or a server.

b. Firewalls cannot be implemented in stand-alone hardware.

c. Increasingly, vendors are refusing to make their firewalls available as virtual appliances.

d. Firewalls are identical when it comes to implementation and ongoing management.

5. The pfSenseFirewallPlanner spreadsheet contains which two worksheets?

a. Configuration Planning and Firewall Planning

b. Physical Configuration and Firewall Rules

c. Firewall Configuration and Physical Rules

d. Firewall Planning and Firewall Wizard

6. The pfSenseFirewallPlanner spreadsheet is designed to document answers to the questions prompted by the:

a. Firewall Planning Wizard.

b. Firewall Administrator.

c. pfSense Firewall Planner.

d. pfSense Firewall Setup Wizard.

7. A(n) \_\_\_\_\_\_\_\_\_\_ is the unique name of the computer on the network capable of originating or responding to an interaction using the Internet Protocol

a. Domain name

b. configuration

c. hostname

d. address

8. Which of the following statements is true regarding the pfSense firewall?

a. The pfSense firewall timestamps log entries.

b. It is not important whether or not firewalls use the correct time and date.

c. It is not possible to correlate logs to security events.

d. In production, a time server should not be used.

9. The process of defining firewall rules can be compared to the process of defining most Access Control Lists (ACLs) because, in both cases, they are:

a. sophisticated programs with conditional branching logic.

b. programs that use a restrictive approach.

c. programs that use a permissive approach.

d. simple lists of rules that are evaluated in order.

10. Which of the following firewall default settings generally makes users happier because everything that they wish to do is allowed?

a. Restrictive

b. Permissive

c. Prohibitive

d. Explicit

11. Which of the following firewall default settings is the preferred approach from a security standpoint, although it requires more thoughtful configuration of the rules?

a. Restrictive

b. Permissive

c. Prohibitive

d. Explicit

12. Which of the following firewall default settings is applied by the pfSense firewall?

a. Restrictive

b. Permissive

c. Prohibitive

d. Explicit

13. Which of the following choices in the Action column of the Firewall Rules worksheet means that the questionable incoming packet is discarded (or logged) and provides no indication to the sender that the packet has not reached the intended destination?

a. Pass

b. Return

c. Reject

d. Block

14. Which of the following choices in the Action column of the Firewall Rules worksheet means that the questionable incoming packet is returned to the sender indicating that the packet or packets they sent were not accepted?

a. Pass

b. Return

c. Reject

d. Block

15. Which of the following columns in the Firewall Rules worksheet enables a rule to be made inactive but not deleted, which can be useful for testing purposes or to temporarily allow a certain action?

a. Action

b. Interface

c. Disabled

d. Source O/S

16. Which of the following columns in the Firewall Rules worksheet enables traffic to be allowed by a certain rule only from specific operating systems and only for Transmission Control Protocol (TCP) traffic?

a. Action

b. Interface

c. Disabled

d. Source O/S

17. In the lab, for which of the following types of traffic did you NOT specify a rule?

a. HTTP

b. HTTPS

c. FTP

d. DNS

18. The File Transfer Protocol (FTP) uses which transport protocol?

a. Simple Mail Transfer Protocol (SMTP)

b. Transmission Control Protocol (TCP)

c. User Datagram Protocol (UDP)

d. Internet Control Message Protocol (ICMP)

19. Which of the following are designed to limit access from a trusted network to an untrusted network?

a. LAN rules

b. WLAN rules

c. Browsing rules

d. firewalls

20. By default, the pfSense firewall \_\_\_\_\_\_\_\_\_\_ outbound access from the LAN interface.

a. allows restricted

b. allows unrestricted

c. allows permissive

d. does not allow any

NAME:

Natnael kebede