**Chapter 9 – Firewalls and Intrusion Prevention Systems**

**TRUE/FALSE QUESTIONS:**

T F 1. The firewall may be a single computer system or a set of two or more

systems that cooperate to perform the firewall function.

T F 2. A firewall can serve as the platform for IPSec.

T F 3. The firewall can protect against attacks that bypass the firewall.

T F 4. A packet filtering firewall is typically configured to filter packets going

in both directions.

T F 5. One disadvantage of a packet filtering firewall is its simplicity.

T F 6. The countermeasure to tiny fragment attacks is to discard packets with

an inside source address if the packet arrives on an external interface.

T F 7. A traditional packet filter makes filtering decisions on an individual

packet basis and does not take into consideration any higher layer context.

T F 8. A prime disadvantage of an application-level gateway is the additional

processing overhead on each connection.

T F 9. The primary role of the personal firewall is to deny unauthorized

remote access to the computer.

T F 10. A DMZ is one of the internal firewalls protecting the bulk of the

enterprise network.

T F 11. A logical means of implementing an IPSec is in a firewall.

T F 12. Distributed firewalls protect against internal attacks and provide

protection tailored to specific machines and applications.

T F 13. An important aspect of a distributed firewall configuration is security

monitoring.

T F 14. Unlike a firewall, an IPS does not block traffic.

T F 15. Snort Inline enables Snort to function as an intrusion prevention

capability.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_ control determines the types of Internet services that can be accessed, inbound or outbound.

A. Behavior B. Direction

C. Service D. User

2. \_\_\_\_\_\_\_\_\_ control controls how particular services are used.

A. Service B. Behavior

C. User D. Direction

3. \_\_\_\_\_\_\_\_\_ control determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

A. Behavior B. User

C. Direction D. Service

4. \_\_\_\_\_\_\_\_ control controls access to a service according to which user is attempting to access it.

A. User B. Direction

C. Service D. Behavior

5. The \_\_\_\_\_\_\_\_\_ defines the transport protocol.

A. destination IP address B. source IP address

C. interface D. IP protocol field

6. A \_\_\_\_\_\_\_\_\_\_ gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

A. packet filtering B. stateful inspection

C. application-level D. circuit-level

7. An example of a circuit-level gateway implementation is the \_\_\_\_\_\_\_\_\_\_ package.

A. application-level B. SOCKS

C. SMTP D. stateful inspection

8. Typically the systems in the \_\_\_\_\_\_\_\_\_ require or foster external connectivity such as a corporate Web site, an e-mail server, or a DNS server.

A. DMZ B. IP protocol field

C. boundary firewall D. VPN

9. A \_\_\_\_\_\_\_\_\_ consists of a set of computers that interconnect by means of a relatively unsecure network and makes use of encryption and special protocols to provide security.

A. proxy B. UTM

C. VPN D. stateful inspection firewall

10. A \_\_\_\_\_\_\_\_\_ configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.

A. packet filtering firewall B. distributed firewall

C. personal firewall D. stateful inspection firewall

11. Typical for SOHO applications, a \_\_\_\_\_\_\_\_\_\_ is a single router between internal and external networks with stateless or full packet filtering.

A. single bastion T B. double bastion inline

C. screening router D. host-resident firewall

12. \_\_\_\_\_\_\_\_\_\_ are attacks that attempt to give ordinary users root access.

A. Privilege-escalation exploits B. Directory transversals

C. File system access D. Modification of system resources

13. \_\_\_\_\_\_\_\_\_\_ scans for attack signatures in the context of a traffic stream rather than individual packets.

A. Pattern matching B. Protocol anomaly

C. Traffic anomaly D. Stateful matching

14. \_\_\_\_\_\_\_\_\_\_ looks for deviation from standards set forth in RFCs.

A. Statistical anomaly B. Protocol anomaly

C. Pattern matching D. Traffic anomaly

15. The \_\_\_\_\_\_\_\_\_ attack is designed to circumvent filtering rules that depend on TCP header information.

A. tiny fragment B. address spoofing

C. source routing D. bastion host

**SHORT ANSWER QUESTIONS:**

1. The \_\_\_\_\_\_\_\_\_ is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter to protect the premises network from Internet-based attacks.
2. A \_\_\_\_\_\_\_\_\_ firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
3. The \_\_\_\_\_\_\_\_ IP address is the IP address of the system that originated the IP packet.
4. An intruder transmitting packets from the outside with a source IP address field containing an address of an internal host is known as IP address \_\_\_\_\_\_\_\_\_.
5. The \_\_\_\_\_\_\_\_\_\_ protocol is an example of a circuit-level gateway implementation that is conceptually a “shim-layer” between the application layer and the transport layer and does not provide network-layer gateway services.
6. Identified as a critical strong point in the network’s security, the \_\_\_\_\_\_\_\_\_ serves as a platform for an application-level or circuit-level gateway.
7. A \_\_\_\_\_\_\_\_\_\_ firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side.
8. A \_\_\_\_\_\_\_\_ uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.
9. \_\_\_\_\_\_\_\_\_\_ protocols operate in networking devices, such as a router or firewall, and will encrypt and compress all traffic going into the WAN and decrypt and uncompress traffic coming from the WAN.
10. A \_\_\_\_\_\_\_\_\_\_\_ makes use of both signature and anomaly detection techniques to identify attacks.
11. \_\_\_\_\_\_\_\_\_ matching scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.
12. \_\_\_\_\_\_\_\_\_\_ anomaly watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.
13. Snort Inline adds three new rule types: drop, reject, and \_\_\_\_\_\_\_\_\_.
14. A single device that integrates a variety of approaches to dealing with network-based attacks is referred to as a \_\_\_\_\_\_\_\_\_\_ system.
15. The firewall follows the classic military doctrine of \_\_\_\_\_\_\_\_\_ because it provides an additional layer of defense.