**Chapter 8 – Intrusion Detection**

**TRUE/FALSE QUESTIONS:**

T F 1. An intruder can also be referred to as a hacker or cracker.

T F 2. Activists are either individuals or members of an organized crime

group with a goal of financial reward.

T F 3. Running a packet sniffer on a workstation to capture usernames and passwords is an example of intrusion.

T F 4. Those who hack into computers do so for the thrill of it or for status.

T F 5. Intruders typically use steps from a common attack methodology.

T F 6. The IDS component responsible for collecting data is the user interface.

T F 7. Intrusion detection is based on the assumption that the behavior of the

intruder differs from that of a legitimate user in ways that can be quantified.

T F 8. The primary purpose of an IDS is to detect intrusions, log suspicious

events, and send alerts.

T F 9. Signature-based approaches attempt to define normal, or expected,

behavior, whereas anomaly approaches attempt to define proper behavior.

T F 10. Anomaly detection is effective against misfeasors.

T F 11. To be of practical use an IDS should detect a substantial percentage of

intrusions while keeping the false alarm rate at an acceptable level.

T F 12. An inline sensor monitors a copy of network traffic; the actual traffic

does not pass through the device.

T F 13. A common location for a NIDS sensor is just inside the external

firewall.

T F 14. Network-based intrusion detection makes use of signature detection

and anomaly detection.

T F 15. Snort can perform intrusion prevention but not intrusion detection.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_ are either individuals or members of a larger group of outsider attackers who are motivated by social or political causes.

A. State-sponsored organizations B. Activists

C. Cyber criminals D. Others

2. A \_\_\_\_\_\_\_\_\_ is a security event that constitutes a security incident in which an intruder gains access to a system without having authorization to do so.

A. intrusion detection B. IDS

C. criminal enterprise D. security intrusion

3. A \_\_\_\_\_\_\_\_\_ monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

A. host-based IDS B. security intrusion

C. network-based IDS D. intrusion detection

4. A \_\_\_\_\_\_\_\_ monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

A. host-based IDS B. security intrusion

C. network-based IDS D. intrusion detection

5. The \_\_\_\_\_\_\_\_ is responsible for determining if an intrusion has occurred.

A. analyzer B. host

C. user interface D. sensor

6. \_\_\_\_\_\_\_\_\_\_ involves an attempt to define a set of rules or attack patterns that can be used to decide if a given behavior is that of an intruder.

A. Profile based detection B. Signature detection

C. Threshold detection D. Anomaly detection

7. \_\_\_\_\_\_\_\_\_ involves the collection of data relating to the behavior of legitimate users over a period of time.

A. Profile based detection B. Signature detection

C. Threshold detection D. Anomaly detection

8. A (n) \_\_\_\_\_\_\_\_\_\_ is a hacker with minimal technical skill who primarily uses existing attack toolkits.

A. Master B. Apprentice

C. Journeyman D. Activist

9. The \_\_\_\_\_\_\_\_\_ module analyzes LAN traffic and reports the results to the central manager.

A. LAN monitor agent B. host agent

C. central manager agent D. architecture agent

10. The purpose of the \_\_\_\_\_\_\_\_ module is to collect data on security related events on the host and transmit these to the central manager.

A. central manager agent B. LAN monitor agent

C. host agent D. architecture agent

11. A(n) \_\_\_\_\_\_\_\_ is inserted into a network segment so that the traffic that it is monitoring must pass through the sensor.

A. passive sensor B. analysis sensor

C. LAN sensor D. inline sensor

12. A(n) \_\_\_\_\_\_\_\_ event is an alert that is generated when the gossip traffic enables a platform to conclude that an attack is under way.

A. PEP B. DDI

C. IDEP D. IDME

13. \_\_\_\_\_\_\_\_\_ is a document that describes the application level protocol for exchanging data between intrusion detection entities.

A. RFC 4767 B. RFC 4766

C. RFC 4765 D. RFC 4764

14. The rule \_\_\_\_\_\_\_ tells Snort what to do when it finds a packet that matches the rule criteria.

A. protocol B. direction

C. action D. destination port

15. The \_\_\_\_\_\_\_ is the ID component that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator.

A. data source B. sensor

C. operator D. analyzer

**SHORT ANSWER QUESTIONS:**

1. The broad classes of intruders are: cyber criminals, state-sponsored organizations, \_\_\_\_\_\_\_\_\_ , and others.
2. A \_\_\_\_\_\_\_\_ is a hacker with sufficient technical skills to modify and extend attack toolkits to use newly discovered vulnerabilities.
3. The \_\_\_\_\_\_\_\_\_ to an IDS enables a user to view output from the system or control the behavior of the system.
4. \_\_\_\_\_\_\_\_\_\_ is a security service that monitors and analyzes system events for the purpose of finding, and providing real-time warning of attempts to access system resources in an unauthorized manner.
5. An IDS comprises three logical components: analyzers, user interface and \_\_\_\_\_.
6. Copying a database containing credit card numbers, viewing sensitive data without authorization, and guessing and cracking passwords are examples of \_\_\_\_\_\_\_\_\_ .
7. \_\_\_\_\_\_\_\_\_ anomaly detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations.
8. \_\_\_\_\_\_\_\_ detection techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
9. \_\_\_\_\_\_\_\_\_ simulate human brain operation with neurons and synapse between them that classify observed data
10. A \_\_\_\_\_\_\_\_ IDS monitors traffic at selected points on a network or interconnected set of networks.
11. The \_\_\_\_\_\_\_\_\_ (RFC 4766) document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF).
12. The functional components of an \_\_\_\_\_\_\_\_\_ are: data source, sensor, analyzer, administration, manager, and operator.
13. The \_\_\_\_\_\_\_\_\_ is the predefined formally documented statement that defines what activities are allowed to take place on an organization’s network or on particular hosts to support the organization’s requirements.
14. \_\_\_\_\_\_\_\_ are decoy systems that are designed to lure a potential attacker away from critical systems.
15. The \_\_\_\_\_\_\_\_\_\_ is the human with overall responsibility for setting the security policy of the organization, and, thus, for decisions about deploying and configuring the IDS.