QUESTION 553

Which of the following are the major categories of IDSs response options?

A. Active responses

B. Passive responses

C. Hybrid

D. All of the choices

Correct Answer: D

QUESTION 554

Alarms and notifications are generated by IDSs to inform users when attacks are detected. The most common form of alarm is:

A. Onscreen alert

B. Email

C. Pager

D. Icq

Correct Answer: A

QUESTION 555

Which of the following is a valid tool that complements IDSs?

A. All of the choices.

B. Padded Cells

C. Vulnerability Analysis Systems

D. Honey Pots

Correct Answer: A

QUESTION 556

A problem with a network-based ID system is that it will not detect attacks against a host made by an intruder who is logged in at which of the following?

A. host’s terminal

B. guest’s terminal

C. client’s terminal

D. server’s terminal

Correct Answer: A

QUESTION 557

When the IDS detect attackers, the attackers are seamlessly transferred to a special host. This method is called:

A. Vulnerability Analysis Systems
B. Padded Cell
C. Honey Pot
D. File Integrity Checker

Correct Answer: B

QUESTION 558

Which of the following is a weakness of both statistical anomaly detection and pattern matching?

A. Lack of ability to scale.
B. Lack of learning model.
C. Inability to run in real time.
D. Requirement to monitor every event.

Correct Answer: B

QUESTION 559

The two most common implementations of Intrusion Detection are which of the following?

A. They commonly reside on a discrete network segment and monitor the traffic on that network segment.
B. They commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
C. They commonly reside on a discrete network segment but do not monitor the traffic on that network segment.
D. They commonly do not reside on a discrete network segment and monitor the traffic on that network segment.

Correct Answer: A

QUESTION 560

What are the primary approaches IDS takes to analyze events to detect attacks?

A. Misuse detection and anomaly detection.
B. Log detection and anomaly detection.
C. Misuse detection and early drop detection.

D. Scan detection and anomaly detection.

Correct Answer: A

QUESTION 561

Misuse detectors analyze system activity and identify patterns. The patterns corresponding to know attacks are called:

A. Attachments
B. Signatures
C. Strings
D. Identifications

Correct Answer: B

QUESTION 562

Which of the following is an obvious disadvantage of deploying misuse detectors?

A. They are costly to setup.
B. They are not accurate.
C. They must be constantly updated with signatures of new attacks.
D. They are costly to use.

Correct Answer: C

QUESTION 563

What detectors identify abnormal unusual behavior on a host or network?

A. None of the choices.
B. Legitimate detectors.
C. Anomaly detectors.
D. Normal detectors.

Correct Answer: C

QUESTION 564

A network-based IDS is which of the following?

A. active while it acquires data
B. passive while it acquires data

C. finite while it acquires data
D. infinite while it acquires data

Correct Answer: B

QUESTION 565

Which of the following usually provides reliable, real-time information without consuming network or host resources?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A

QUESTION 566

Which of the following would assist in intrusion detection?

A. audit trails
B. access control lists
C. security clearances
D. host-based authentication

Correct Answer: A

QUESTION 567

Using clipping levels refers to:

A. setting allowable thresholds on reported activity
B. limiting access to top management staff
C. setting personnel authority limits based on need-to-know basis
D. encryption of data so that it cannot be stolen

Correct Answer: A

QUESTION 568

In what way can violation clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.

B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.

C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to usercodes with a privileged status.

D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to usercodes which have incurred violations.

Correct Answer: A

QUESTION 569

When establishing a violation tracking and analysis process, which one of the following parameters is used to keep the quantity of data to manageable levels?

A. Quantity baseline

B. Maximum log size

C. Circular logging

D. Clipping levels

Correct Answer: D

QUESTION 570

Audit trails based upon access and identification codes establish

A. intrusion detection thresholds

B. individual accountability

C. audit review criteria

D. individual authentication

Correct Answer: B

QUESTION 571

The primary reason for enabling software audit trails is which of the following?

A. Improve system efficiency.

B. Improve response time for users.

C. Establish responsibility and accountability.