


QUESTION 1 OF 10

What is a profiling technique that monitors how applications use resources called?

Choose only ONE best answer.

- A System monitoring
- B Resource profiling
- C Application monitoring
- D Executable profiling** 

This answer is correct.

NEXT

QUESTION 2 OF 10

IDS is an acronym for:

Choose only ONE best answer.

A Intrusion-detection system



B Intrusion-deterrence system

C Intrusion-deterrence service

D Intrusion detection service

This answer is correct.

QUESTION 3 OF 10

What is another term for preemptive blocking?

Choose only ONE best answer.

A Intrusion detection

B Banishment vigilance



C User deflection

D Intruder blocking

This answer is correct.

QUESTION 4 OF 10

What is an attempt to attract intruders to a system setup for monitoring them called?

Choose only ONE best answer.

A Intrusion deterrence

B Intrusion detection 

C Intrusion banishment


D Intrusion routing

This answer is correct.

QUESTION 5 OF 10

What type of IDS is Snort?

Choose only ONE best answer.


- A** Router based
- B** Operating system based
- C** Host based 
- D** Client based

This answer is correct.

QUESTION 6 OF 10

Specter aggressive mode tries to trace the attacker and gain its identity

Choose only ONE best answer.

- A** True 
- B** False

This answer is correct.

QUESTION 7 OF 10

Specter is an advanced IDS system

Choose only ONE best answer.

A True



B False

This answer is incorrect.

QUESTION 8 OF 10

What is a system that is setup for attracking and monitoring intruders called?

Choose only ONE best answer.

A Fly paper

B Trap door

C Honeypot



D Hacker cage

This answer is correct.

QUESTION 9 OF 10

Which of the following is NOT a profiling strategy used in anomaly detection?

Choose only ONE best answer.

A Threshold monitoring

B Resource profiling

C Executable profiling



D System monitoring

This answer is incorrect.

QUESTION 10 OF 10

What could a series of ICMP packets sent to your ports in sequence indicate?

Choose only ONE best answer.

A A DoS attack

B A ping flood 

C A packet sniffer

D A port scan

This answer is correct.