1. What are the different ways to intrude?

Crt ans: a) Buffer overflows  
b) Unexpected combinations and unhandled input  
c) Race conditions

1. What are the major components of the intrusion detection system?

Crt ans: a) Analysis Engine  
b) Event provider  
c) Alert Database

1. What are the different ways to classify an IDS?

Crt ans: Host & Network based

Wrng ans: Network & Zone based

1. What is the major drawback of anomaly detection IDS?

Crt ans: It generates many false alarms

Wrng ans: It doesn’t detect novel attacks

1. What are characteristics of Network based IDS?

Crt ans: They look for attack signatures in network traffic

Wrng ans: It is programmed to interpret a certain series of packet

1. AP is abbreviated as \_\_\_\_\_\_\_\_\_\_\_\_\_.

Crt ans: Access Point

Wrng ans: Access Position