Tutorial Week 7 Solutions (abbreviated)

Questions

3. An organisation uses Probabilistic Packet Marking to trace sources of attacks. It receives a large number of packets with the following information:

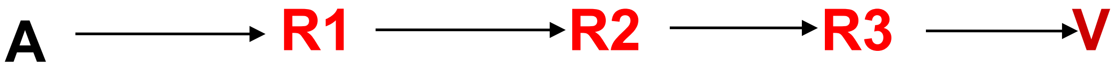
3	AB
2	BC
1	CD
2	EC

Reconstruct the path or paths taken by the attack packets.

Attacker-A-B-C-D-Victim and

Attacker-E-C-D-Victim

4. Consider the following diagram showing a flow of packets from an attacker to a victim via routers R1, R2 and R3.



Routers R1, R2 and R3 all use PPM.

What will be the contents of the ID field if:

a. R1 marks the packet, R2 marks the packet and R3 does not mark the packet

   1, R2R3

b. R1 does not mark the packet, R2 marks the packet and R3 does not mark the packet

   1, R2R3

c. R1 does not mark the packet, R2 does not mark the packet and R3 marks the packet

   0, R3,-

d. R1 marks the packet, R2 does not mark the packet and R3 does not mark the packet

   2, R1R2