Tutorial Week 7

Questions

1. An organisation uses Node Sampling to identify the source of DDoS attacks. It receives a large number of packets marked with router ids in approximately the following ratio. All routers use the same marking probability.

Router A: 25%

Router B: 6.25%

Router C: 50%

Router D: 12.5%

Unmarked: 6.25%

What marking probability is used by the routers?

What is the probable path (or paths) of attack packets?

2. An organisation uses Node Sampling to trace sources of attacks through its routers A, B, C, D, E. Each router marks a packet with probability 0.5. What will be the percentage of packets marked with A, B, C, D, E and unmarked at V? Assume traffic volumes on ACE the same as BDE.

```
A - C
     \
      E - V
     /
B - D
```

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

AB 3

BC 2

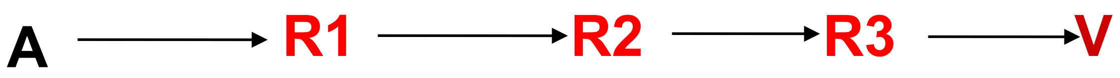
CD 1

EC 2

Reconstruct the path or paths taken by the attack packets.

Tutorial Week 7

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 at the victim if:

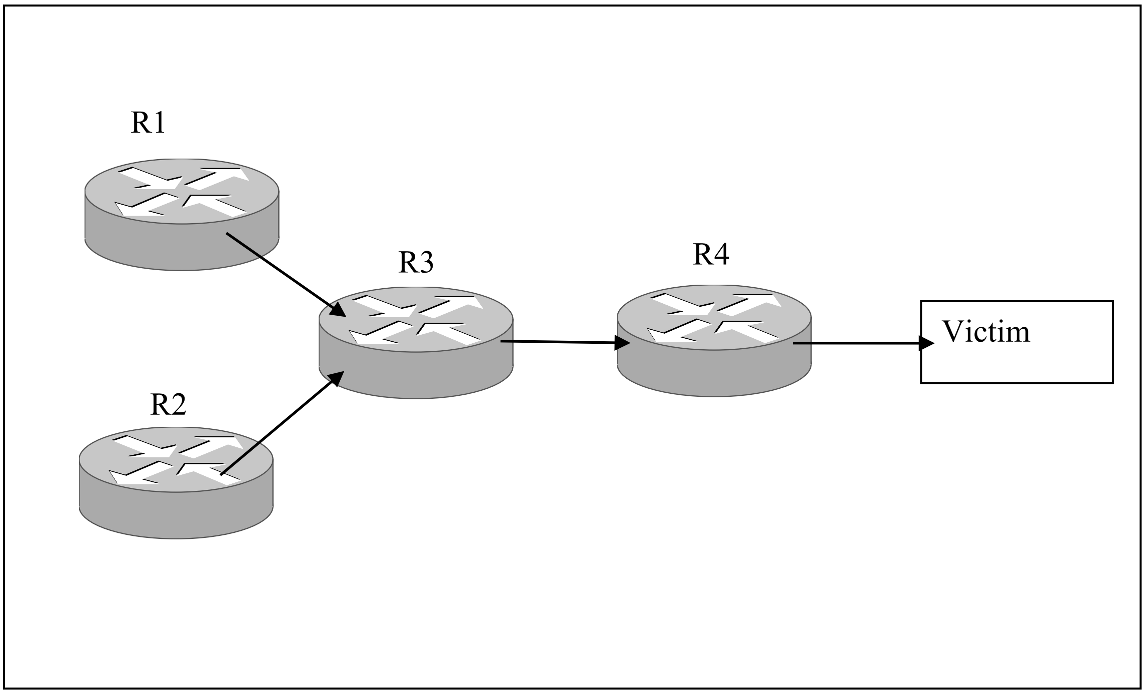
a. R1 marks the packet, R2 marks the packet and R3 does not mark the packet

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

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

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

Tutorial Week 7



5. Referring to the above diagram, R2 marks a packet. No other router marks it.

    a. What will be the value of the ID field when it arrives at R3?
    b. What will be the value of the ID field when it leaves R3?
    c. What will be the value of the ID field when it arrives at R4?
    d. What will be the value of the ID field when it leaves R4?

6. Referring to the above diagram, R1 marks a packet. R3 marks the same packet. No other router marks it.

    a. What will be the value of the ID field when it arrives at R3?
    b. What will be the value of the ID field when it leaves R3?
    c. What will be the value of the ID field when it arrives at R4?
    d. What will be the value of the ID field when it leaves R4?

7. Referring to the above diagram, R4 marks a packet.

    a. What will be the value of the ID field when it arrives at the victim?