Muzaffarpur Institute of Technology, Muzaffarpur

Department of Information Technology

Intrusion Detection System

Mid Term Paper Solution

Question: As a network engineer you designed a network in an IT Lab. Answer the following question if you figured out there may be an intrusion in your network with the following packet. [Information is given in Hexadecimal form and the data carried by this packet should be converted using ASCII value].

45 00 00 2E B5 73 40 00 40 06 85 BC 7F 00 00 02 7F 80 00 22 AB 42 00 50 59 64 A6 1C 02 B3 D3 6C 50 18 01 18 01 56 FF BA 00 00 4D 49 54 49 41 4E

a) Write the Source & Destination IP Address (Write in proper decimal form).
b) Which application layer protocol's data is being carried out.
c) What is the length of actual data.
d) How long this packet is going to live before reaching destination.
e) What will happen to this packet if it reaches a link with a smaller MTU than this packet size? Answer with justification in maximum 3 sentences

Answer:

i) Write the Source & Destination IP Address (Write in proper decimal form)
Ans: Source Address: **7F 00 00 02 i.e. 127.0.0.2**
Destination Address: **7F 80 00 22 i.e. 127.128.0.34**

ii) Which application layer protocol's data is being carried out
Ans: Source Port Number: **AB 42 i.e. 43842**
Destination Port Number: **00 50 i.e. 80**
As we know 80 is the port number used for web service, so the application layer protocol HTTP.

iii) What is the length of actual data
Ans: From IP header we can find out, IP header length is 5*4 =20 Bytes, Total Length is 00 2E i.e. 46 Bytes. Hence the actual payload of IP packet is 46 - 20 = 26 Bytes. This 26 Bytes includes TCP header and actual Data. From TCP header we can see that the header size is **5** * 4 = 20 Bytes, so the actual data is 46 – 20 = 6 Bytes (**4D 49 54 49 41 4E)**

iv) How long this packet is going to live before reaching destination
Ans: TTL Value is **40 i.e.** 64. It is going to live 60 jumps/hops/network jumps.

v) What will happen to this packet if it reaches a link with a smaller MTU than this packet size? Answer with justification in maximum 3 sentences.
Ans: From the header information about Flag + Fragmentation offset (**40 00**) (Binary form: 0100 0000 0000 0000), we can see that the 1st three bits are **010** and we know that it is used for making fragmentation decision. Here D (2nd Bit) = 1 & M (3dr Bit) = 0. So the packet can't be fragmented and hence **discarded** from network.