NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 1

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following statement(s) is/are true with respect to penetration testing of a network?

a. In the white box model, the tester has complete information about the network.
b. In the black box model, the tester has complete information about the network.
c. In the gray box model, the tester has partial information about the network.
d. In the red box model, the tester does not have any information about the network.

Correct Answer: a, c

Detail Solution: In the white box model, the tester has complete information about the network. In the black box model, the tester does not have any information about the network. Gray box model is somewhere in between, where the tester is only provided with partial information about the network. There is nothing called red box model.

QUESTION 2:

Which of the following statement(s) is/are true for a packet switched network?

a. A point-to-point communication link may be shared by more than one end-to-end connection.
b. A point-to-point communication link is dedicated to a connection and cannot be shared with other connections.
c. The packet transfer delay between a pair of nodes is more or less constant during the entire period of the connection.
d. The packet transfer delay between a pair of nodes may depend on the prevailing network traffic.

Correct Answer: a, d

Detail Solution: In a circuit switched network, a communication link remains dedicated to a connection; however, in a packet switched network, communication links may be shared by more than one connection. Also, in a packet switched network, packets between the same source and destination may follow different paths, and hence the packet transfer delay can vary with time; this depends on the prevailing traffic situation in the network. Thus, options (a) and (d) are true.

QUESTION 3:

A packet of size 5000 bytes is sent over a 100 kilo-bits-per-second (Kbps) point-to-point link whose propagation delay is 5 msec. The packet will reach the destination after _____ msec. (Assume 1K = 1000)

Correct Answer: 400 to 405

Detail Solution: 100x1000 = 100,000 bits per second can be transferred through the link.

1 bit can be sent in = (1 / 100,000) sec

5000 bytes or 40,000 bits can be sent in 40,000 / 100,000 sec = 0.40 sec = 400 msec

Hence the packet will reach the destination after = 400 msec + 5 msec = 405 msec

---

QUESTION 4:

Which of the following OSI layers is responsible for node-to-node routing of packets?

a. Physical layer
b. Transport layer
c. Network layer
d. Datalink layer

Correct Answer: c

Detail Solution: The physical layer is responsible for actual transmission of signals over a communication medium. The data-link layer is responsible for transmitting data frames reliably over point-to-point links. The network layer is responsible for the switching or routing of packets from one node to the next on way to its final destination. The transport layer is a virtual host-to-host layer between the two end systems. Thus, the correct option is (c).

QUESTION 5:

What is the purpose of the port number in TCP/IP networks?

a. It uniquely identifies a network interface of a computer system.
b. It uniquely identifies a host in the network.
c. It indicates how many hardware ports are there in the computer system.
d. None of these.

Correct Answer: d

Detail Solution: Port number uniquely identifies a running application on a specified host in the network. The correct option is (d).

QUESTION 6:

Which of the following statement(s) is/are true for the TCP protocol?

a. It provides connection-oriented, reliable packet transfer service.
b. It provides connection-less datagram service.
c. All packets from a source to a destination follow the same path.
d. It routes the packets from one node to the next.

Correct Answer: a

Detail Solution: TCP ensures connection-oriented and reliable message transfer service between two hosts. However, it runs on top of the IP protocol for packet delivery, which is a datagram based service and hence individual packets constituting the message may follow different paths. Also, it is not responsible for routing of the packets. Hence, the correct option is (a).

QUESTION 7:

Which of the following are valid port numbers in TCP/IP?

a. 10,000
b. 50,000
c. 100,000
d. 500,000
e. 750,000

Correct Answer: a, b

Detail Solution: In TCP/IP, port numbers are 16-bit quantities, with values in the range of 0 to 2^{16}-1 = 65535. Hence, the correct options are (a) and (b).

QUESTION 8:

If the IP header is 256 bits long, what will be the value of the "HLEN" field?

a. 4
b. 5
c. 16
d. 24
e. None of these

Correct Answer: e

Detail Solution: The HLEN field contains the size of the IP header in multiples of 32 bits or 4 bytes. Here, size of the IP header = 256 bits = 8 x 32 bits. Hence, HLEN will contain 1000, which is the binary equivalent of the number 8. Thus, the correct option is (e).

QUESTION 9:

The maximum size of data that can be accommodated in an IP datagram is _____ bytes.

Correct Answer: 65500 to 65535

Detail Solution: The TOTAL-LENGTH field in the IP header is 16 bits, which can contain values from 0 to $2^{16} – 1$ = 65535, the total size of an IP packet can be 65535 bytes. Also, the minimum size of the IP header is 20 bytes, which makes the maximum size of data as 65535 – 20 = 65515 bytes.

QUESTION 10:

Which of the following statement(s) is/are true?

a. For small number of packets, datagram is faster than virtual circuits.
b. For large number of packets, datagram is faster than virtual circuits.
c. In datagram, a dedicated communication path is established between two end stations.

d. In datagram, it is not required to establish a connection between two end systems.

Correct Answer: a, d

Detail Solution: Virtual circuits have the initial overhead of connection establishment, but once it is done, packets will flow faster as the header size is smaller. Datagrams do not require connection establishment. For less number of packets, the overhead will dominate, and hence datagram will be faster. For large number of packets, however, virtual circuit will become faster as the overhead per packet becomes less. Also, in circuit switching, a dedicated communication path is established between two end stations; while in virtual circuits, no such dedicated path is established. Hence, the correct options are (a) and (d).

**********END*******