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*******

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment- Week 2

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

An IP packet arrives at a router with the first eight bits as 01001101. How many bytes are there in the OPTIONS field?

a. 4
b. 8
c. 12
d. 16
e. None of these

**Correct Answer: e**

**Detail Solution:** The first four bits (0100) is the IP version, and the next four bits (1101 = 13) is the header length. The header length of 13 indicates 13 x 4 = 52 bytes of header. The basic IP header is 20 bytes long. Hence, the size of the OPTIONS field will be 52 – 20 = 32 bytes. The correct option is (e).

---

**QUESTION 2:**

In an IP packet, the value of HLEN is 8, and the value of the TOTAL LENGTH field is 1500 (in decimal). The number of data bytes in the packet will be _____

**Correct Answer: 1450 to 1475**

**Detail Solution:** Since HLEN = 8, the size of the IP header will be 8 x 4 = 32 bytes. The total size of the IP packet is given as 1500 bytes. Hence, the number of data bytes = 1500 – 32 = 1468 bytes.

---

**QUESTION 3:**

An IP packet arrives at the final destination with the M flag set as 1. Which of the following statement(s) is/are true about the packet?

a. The packet represents a fragment of a larger packet.
b. The packet will be fragmented by the next router.
c. The packet is the first of multiple fragments.
d. None of these.

**Correct Answer: a**

**Detail Solution:** When the Mode (M) flag in a packet is 1, this indicates that the original packet has definitely been fragmented. Also, this is not the last fragment … there are more fragments after this. Hence, option (a) is true.

---

**QUESTION 4:**

Which address classes do the IP addresses 144.16.75.12 and 10.10.85.120 belong to?

a. Class C and Class A
b. Class B and Class C
c. Class B and Class A
d. Class B and Class D

**Correct Answer: c**

**Detail Solution:** Class A addresses start with "0", class B addresses start with "10", class C addresses start with "110", and class D addresses start with "1110". For the IP address 144.16.75.12, the first byte 144 = **10**010000 in binary; for the IP address 10.10.85.120, the first byte 10 = **0**000 1010 in binary. Clearly, the first one in Class B, and the second one is Class A. Hence. The correct option is (c).

---

**QUESTION 5:**

Which of the following IP addresses represent broadcast address?

a. 144.16.255.255
b. 144.16.0.255
c. 202.0.255.0
d. 202.0.255.255

**Correct Answer: a, d**

**Detail Solution:** In a broadcast address, all the bits in the "host" part of the IP address will be 1. (a) and (b) are class B addresses, where the last 16 bits indicate the host. (c) and (d) are class C addresses, where the last 8 bits indicate the host. Hence, the correct options are (a) and (d).

---

**QUESTION 6:**

What happens when an IP packet gets fragmented?

a. The total number of bits transmitted over the network decreases.
b. The total number of bits transmitted over the network increases.
c. The total number of bits transmitted over the network remains the same as compared to the non-fragmented case.
d. None of these.

**Correct Answer: b**

**Detail Solution:** Each IP fragment will have a header of 20 bytes. Thus more the number of fragments, the overhead of the IP headers will increase. Hence, the total number of bits transmitted will increase. The correct option is (b).

---

**QUESTION 7:**

The maximum number of hosts that are possible in a class B network is _____

**Correct Answer: 65534**

**Detail Solution:** For a class B network, 16 bits are provided to specify the host. The all-0 and all-1 combinations cannot be used as host addresses. Therefore, the maximum number of hosts possible is $2^{16} - 2 = 65534$.

---

**QUESTION 8:**

What is the purpose of the port number field in the TCP header?

a. It indicates the sequence number of the message.
b. In indicates the hardware port of the destination host.
c. It indicates the hardware port of the source host.
d. None of these.

**Correct Answer: d**

**Detail Solution:** In the TCP and UDP protocols, the 16-bit port number uniquely identifies an application running on the host. Two port numbers are specified, source port and destination port. Hence, the correct option is (d).

---

**QUESTION 9:**

What is the subnet address if the destination IP address is 144.16.75.105 and the subnet mask is 255.255.240.0?

a. 144.16.32.0
b. 144.16.75.0
c. 144.16.16.0
d. None of these

**Correct Answer: a**

**Detail Solution:** Let us express the two numbers in binary:

```
144.16.75.105   =  10010000 00010000 00101011 01101001
255.255.240.0   =  11111111 11111111 11110000 00000000
```

If we take bit-by-bit AND, we shall get the subnet address as

```
10010000 00010000 00100000 00000000 = 144.16.32.0
```

---

**QUESTION 10:**

What is a TCP half-open connection in the context of connection establishment using 3-way handshake?

a. The first transaction does not complete.
b. The second transaction does not complete.
c. The first transaction does not complete but the second transaction completes.
d. The last transaction does not complete.
e. None of these.

**Correct Answer: d**

**Detail Solution:** In the TCP protocol, connection establishment is carried out using a 3-way handshake protocol. When the third transaction in the 3-way handshake does not complete, it is referred to as a half-open connection. The correct option is (d).

---

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment- Week 3

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

Which of the following is/are true for *direct packet delivery* option in a routing table?

a. Based on the destination IP address, the packet will be forwarded for processing to another router.
b. Based on the destination IP address, the packet will be forwarded for processing to the default router.
c. Based on the destination IP address, the packet is forwarded to the destination host present in the same network.
d. None of these.

**Correct Answer: c**

**Detail Solution:** Direct packet delivery means that a packet can be delivered to a host directly without going through any other intermediate router. This is possible only when the destination host is present in the same network. Hence, the correct option is (c).

---

**QUESTION 2:**

Which of the following host address represents the default route in a routing table?

a. 0.0.0.1
b. 255.255.255.255
c. 127.0.0.1
d. None of these

**Correct Answer: d**

**Detail Solution:** In the routing table entry of a router, the all-zero combination (0.0.0.0) is typically used to specify the default route.

Hence, option (d) is correct.

---

**QUESTION 3:**

What does the value 1 in the G flag of a routing table signify?

a. The hop count of the packet has expired.
b. The destination is in the same network.
c. The destination is in a different network.
d. The destination is under the default router.
e. None of these.

**Correct Answer: c**

**Detail Solution:** If in a routing table entry, G = 0, it indicates that the destination is in the same network. However, if G = 1, it indicates that the destination is in a different network. In other words, the G flag indicates that the destination is in a different network. Hence, the correct option is (c).

---

**QUESTION 4:**

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

a. All the participating routers are present in the same autonomous system.
b. The participating routers are present in different autonomous systems.
c. Routers in different autonomous systems exchange messages to update their routing tables.
d. Routers in the same autonomous system exchange messages to update their routing tables.

**Correct Answer: a, d**

**Detail Solution:** The interior routing protocols applies to a single autonomous system. All the routers inside the AS exchange messages using some standard protocol (e.g. RIP or OSPF) and update their routing tables. The correct options are (a) and (d).

---

**QUESTION 5:**

If a packet is to be delivered to exactly one within a given set of hosts in a network, what kind of address should be used to specify the destination?

a. Unicast address

b. Broadcast address
c. Anycast address
d. None of these

**Correct Answer: c**

**Detail Solution:** Unicast address is used if a packet is to be delivered to a specific host. Broadcast address is used if a packet has to be delivered to all the hosts within a network or subnetwork. Anycast address is used if a packet has to be delivered to exactly one of the hosts in a network or subnetwork. Hence, the correct option is (c).

---

**QUESTION 6:**

How is the destination network address determined while finding a match in the routing table?

a. Perform bitwise-AND of the destination IP address of the packet with subnet mask entry in the routing table.
b. Perform bitwise-AND of the destination IP address of the packet with network address entry in the routing table.
c. Destination network address can be obtained directly from the information present in the packet.
d. None of these.

**Correct Answer: a**

**Detail Solution:** While finding a match in the routing table, the router first extracts the destination IP address from the incoming packet, and then carries out bitwise-AND operation with the subnet mask entries present in the routing table. The correct option is (a).

---

**QUESTION 7:**

How are the links between neighbor routers kept alive in the OSPF protocol?

a. By sending PING request.
b. By initiating a TCP 3-way handshake protocol.
c. By periodically sending link-state information.
d. By periodically sending HELLO packets.

**Correct Answer: d**

**Detail Solution:** A HELLO packet received from a neighboring router indicates that the corresponding communication link is up and running. In the OSPF protocol, if the HELLO packet is not received for 40 seconds, it indicates failure of the neighbor or the communication link. Hence the correct option is (d).

---

**QUESTION 8:**

Which of the following represents tunneling?

a. An entire IPv6 packet is included as payload inside an IPv4 packet.
b. A packet is sent from an IPv4 network to an IPv6 network.
c. A packet is sent from an IPv6 network to an IPv4 network.
d. None of these.

**Correct Answer: a**

**Detail Answer:** When entire IPv6 packets are encapsulated within IPv4 packets, it is called tunneling. The IPv6 packet gets transmitted as data over an IPv4 network. Hence, the correct option is (a).

---

**QUESTION 9:**

Consider the following routing table in a router. On which interface will an IP packet with destination address 161.44.64.120 be forwarded?

| Destination | Subnet Mask | Interface |
|---|---|---|
| 161.44.0.0 | 255.255.0.0 | a |
| 161.44.64.0 | 255.255.224.0 | b |
| 161.44.68.0 | 255.255.255.0 | c |
| 161.44.68.64 | 255.255.255.224 | d |
| default | 0.0.0.0 | e |

a. Interface a
b. Interface b

c. Interface c
d. Interface d
e. Interface e

**Correct Answer: b**

**Detail Solution:**

Row 1: 161.44.64.120 AND 255.255.0.0 = 161.44.0.0 ➔ Matches with destination address

Row 2: 161.44.64.120 AND 255.255.224.0 = 161.44.64.0 ➔ Matches with destination address

Row 3: 161.44.64.120 AND 255.255.255.0 = 161.44.64.0 ➔ No match

Row 4: 161.44.64.120 AND 255.255.255.224 = 161.44.64.112 ➔ No match

Row 2 provides the longest prefix match; hence the packet will be forwarded to Interface b.

Hence, the correct option is (b).

---

**QUESTION 10:**

An entry in the routing table has 155.86.56.0 as the destination, and /22 as the subnet mask. What will be the network address?

a. 155.86.56.0
b. 155.86.0.0
c. 155.86.48.0
d. None of these.

**Correct Answer: a**

**Detail Solution:** In binary notation,

155.86.56.0 = 10011011 01010110 00111000 00000000

If we use /22 as the subnet mask, this means that the first 22 bits of the address must be used to get the network address. If we do this, we get

10011011 01010110 00111000 00000000 = 155.86.56.0

Hence, correct option is (a).

---

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

# Ethical Hacking

## Assignment- Week 4

### TYPE OF QUESTION: MCQ/MSQ

**Number of questions**: 20 **Total mark: 20 x 0.5 = 10**

---

**QUESTION 1:**

What is the purpose of the Hypervisor software?

a. It is a secure software layer that is difficult to hack.
b. It opens a terminal window through which commands can be given directly.
c. It can create and run multiple virtual machines on a computer system.
d. None of these.

**Correct Answer: c**

**Detailed Solution:**

Hypervisor or Virtual Machine Monitor is a software tool that allows the creation and running of one or more virtual machines (VMs) on a computer system. This is very essential for security practice.

The correct option is (c).

---

**QUESTION 2:**

What are some of the features in Kali Linux?

a. It is a secure operating system that has been designed as hack-proof.
b. It is a Debian-based Linux distribution that have collection of tools that are useful for penetration testing.
c. It is a software distribution created by the company Kali Inc.
d. None of these.

**Correct Answer: b**

**Detailed Solution:** Kali Linux is a specific Linux distribution based on Debian. It consists of a large collection of tools for carrying out penetration testing, security research, computer forensics, etc.

The correct option is (b).

---

**QUESTION 3:**

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

a. Information about the target is collected indirectly.
b. Information about the target is collected directly.
c. There is no direct communication with the target system.
d. There is direct communication with the target system.

**Correct Answer: a, c**

**Detailed Solution:** Reconnaissance is the process of gathering information about a target network or system. In passive reconnaissance, we collect information about a target indirectly without direct communication with the target system.

The correct options are (a) and (c).

---

**QUESTION 4:**

Which of the following can be used for passive reconnaissance?

a. Whois
b. archive.org
c. Netcraft
d. Search engines

**Correct Answer: a, b, c, d**

**Detailed Solution:** All the four options as mentioned can be used for passive reconnaissance, in gathering information about a target indirectly.

---

**QUESTION 5:**

How host discovery can be carried out using ICMP sweep?

a. The attacker sends out an ICMP ECHO request packet to the target, and waits for an ICMP ECHO reply response.
b. It uses ICMP protocol to broadcast packets to all the machines in a network.
c. It utilizes the vulnerability of TCT connection establishment.
d. None of these.

**Correct Answer: a**

**Detailed Solution:** In ICMP sweep, the attacker sends out an ICMP ECHO request packet (ICMP type 8) to the target. If it receives an ICMP ECHO reply packet, it assumes that the target is alive.

The correct option is (a).

---

**QUESTION 6:**

How does port scanning using TCP Connect works?

a. It creates a half-open connection during TCP connection establishment, and decides whether the port is open.
b. It completes the 3-way handshake in TCP connection establishment, and decides whether the port is open.
c. It drops TCP packets as they arrive from the target.
d. None of these.

**Correct Answer: b**

**Detailed Solution:** In TCP Connect, the attacker tries to complete a TCP connection with the target by using 3-way handshake. If successful, it concludes that the given port is open.

The correct option is (b).

---

**QUESTION 7:**

The establishment of a TCP connection involves a negotiation called 3-way handshake. What type of message the client sends to the server in order to begin this negotiation?

a. RST
b. ACK
c. SYN-ACK
d. SYN

**Correct Answer: d**

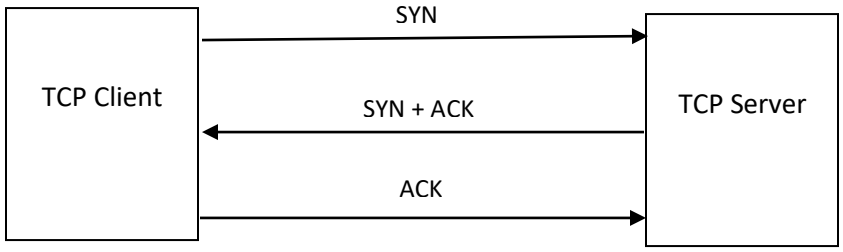
**Detailed Solution:** TCP connection establishment involves a 3-way handshake.

**Step 1 (SYN):** In the first step, client wants to establish a connection with server, so it sends a segment with SYN that informs server that client is likely to start communication and with what sequence number it starts the segments with.

**Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with.

**Step 3 (ACK):** In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start actual data transfer.

The correct option is (d).




**QUESTION 8:**

Which of the following statement(s) is/are true for default networking mode of Oracle Virtual Box?

a. It allocates unique IP addresses to all operating systems.
b. It allocates a virtual IP address to all operating systems.
c. It allocates IP address of the HOST system to all operating systems.
d. In this mode an operating system can access internet
e. None of these.

**Correct Answer: b, d**

**Detailed Solution:** The default networking mode allocated to each operating system by virtual box is NAT, which allocates a same virtual IP address to all operating system. However, in this mode, operating systems can access the internet. The correct options are (b) and (d).

**QUESTION 9:**

Which of the following can be used to retrieve the deleted data and all pages available with any website?

a. Whois
b. archive.org
c. Netcraft
d. Search engines

**Correct Answer: b**

**Detailed Solution:** With the help of archive.org we can interact with older version of the website to retrieve the deleted information. It also provides a functionality to find out all associated pages with the website (host).

The correct option is (b).

---

**QUESTION 10:**

Which of the following search operators can narrow down the search results to a specific website?

a. inurl
b. OR
c. AND
d. site
e. filetype

**Correct Answer: d**

**Detailed Solution:** inurl search operator is used to search all websites that contain the given term as a part of its url. OR and AND operators are used simply as logical OR and AND to show result for both keywords or either. Site operators is used to restrict the search to a particular website. Filetype operator is used to search particular files (i.e. ppt, pdf).

The correct option is (d).

---

**QUESTION 11:**

What is the purpose of the following NMAP command?

```
nmap –sn 192.55.70.110-120
```

a. A trace sweep
b. A ping scan
c. A port scan
d. None of these

**Correct Answer**: b

**Detail Solution**: The –sn options tells nmap not to carry out a port scan after host discovery, and only provide a list of the available hosts that respond to the scan. Basically, only a ping scan is performed.

Thus, the correct option is (b).

---

**QUESTION 12:**

In port scanning using TCP SYN scan, how are the open and closed ports identified?

a. An attacker sends a SYN packet to a port, if it receives an SYN-ACK (SA) then the port is reported as open.
b. An attacker sends a SYN packet to a port, if it receives an RST (RA) then the port is reported as closed.
c. An attacker sends an ACK packet to a port, if it receives an RST then the port is reported as open.
d. An attacker sends an ACK packet to a port, if it receives an RST then the port is reported as closed.

**Correct Answer: a, b**

**Detailed Solution:** in TCP SYN scan open and closed ports are identified by sending SYN request to various ports of the target system. If a SYN-ACK packet is received for a port then the port is reported as open, whereas if it receives a RST (RA) packet then the port is reported as closed. ACK packets are not used in TCP SYN scan.

The correct options are (a) and (b).

---

**QUESTION 13:**

By default how many ports are scanned in nmap for a target system ……?

**Correct Answer: 1000**

**Detailed Solution:** By default nmap scans for top 1000 ports.

---

**QUESTION 14:**

Which of the following options can be used for OS and Version detection?

a. –sn
b. -Pn
c. -A
d. –sT
e. None of these

**Correct Answer: c**

**Detailed Solution:** for OS and version detection –o and –sV option is used. However scanning with option –A, which is known as aggressive scan, performs various type of scanning such as port scanning, host scanning, OS and version detection, vulnerabilities, etc.

The correct option is (c).

---

**QUESTION 15:**

Which of the following nmap option can be used to carry out UDP scan?

a. -sP
b. -sS
c. -sU
d. None of these

**Correct Answer**: c

**Detail Solution**: The –sP option is used for ping scan, -sS option is used for stealth scan, and –sU option is used for UDP scan.

Thus, the correct option is (c).

---

**QUESTION 16:**

For port scanning using stealth scan (-sS), NMAP first identifies if the system is up or not by sending TCP SYN, TCP ACK, and ICMP type-8 packet to target system. Which of the following option can be used along with –sS option to directly start port scanning?

a. -sn
b. -p
c. -Pn
d. None of these

**Correct Answer: c**

**Detailed Solution:** If we give -Pn option along with –sS option then NMAP will ignore host detection (will assume the host is up) and will directly start scanning of ports.

The correct option is (c).

---

**QUESTION 17:**

Which of the following NMAP scanning options will scan less number of ports as compared to default scanning?

a. -F
b. -p20-100
c. -p22, 23, 80, 8080
d. None of these

**Correct Answer: a, b, c**

**Detailed Solution:** By default NMAP scans for 1000 ports. If we want to restrict this, we can directly give the specific port numbers that need to be scanned or we can give range of ports. We can give option F that scans top 100 ports. So option (a) will scan 100 ports, option (b) will scan 82 ports, option (c) will scan 4 ports. There is one more port scanning option that is (-p-), which scans all ports (0 to 65535).

The correct options are (a), (b) and (c).

---

**QUESTION 18:**

Let us say port numbers 80 and 443 are open for a target system. Then there is high probability that the target is hosting a website?

a. True
b. False

**Correct Answer: a**

**Detailed Solution:** In general, a system that is hosting a website keeps port 80 and 443 open. Thus the statement is true.

---

**QUESTION 19:**

Can the use of firewall prevent port/host scanning?

a. True
b. False

**Correct Answer: a**

**Detailed Solution:** Use of firewalls (inbuilt as well as software firewall) can protect you to prevent port/host scanning. We have already done demonstration for this.

---

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment- Week 5

### TYPE OF QUESTION: MCQ/MSQ/SA

**Number of questions**: 15 **Total mark: 15 x 1 = 15**

---

**QUESTION 1:**

Which of the following tools can be used for scanning vulnerabilities?

a. Hypervisor
b. Nessus
c. Hydra
d. Nmap

**Correct Answer**: b, d

**Detail Solution**: The typical tools that are used for scanning vulnerabilities in hosts and networks are NMAP, Nessus, Nexpose, MPSA, etc.

The correct options are (b) and (d).

---

**QUESTION 2:**

Which of the following may be used for password cracking?

a. Dictionary attack.
b. Social engineering attack.
c. TCP SYN attack.
d. DoS attack.

**Correct Answer**: a, b

**Detail Solution**: Dictionary attack and social engineering attacks can be used for cracking passwords. TCP SYN and DoS attacks are typically used to limit the accessibility of a target system.

---

**QUESTION 3:**

Which of the following can be used for gaining higher privileges than existing one?

a. Vertical privilege escalation.
b. Horizontal privilege escalation.
c. Diagonal privilege escalation.
d. None of these.

**Correct Answer**: a

**Detail Solution**: Vertical privilege escalation refers to gaining higher than existing privileges. Horizontal privilege escalation refers to acquiring the same level of privilege with the identity of some other user. There is nothing called diagonal privilege escalation.

The correct option is (a).

---

## QUESTION 4:

Which of the following can self-replicate itself?

a. Trojan
b. Virus
c. Ransomware
d. All of these

**Correct Answer**: b

**Detail Solution**: Virus and worms typically replicate themselves and get attached to other files.

The correct option is (b).

---

## QUESTION 5:

Which of the following can be performed using the NMAP tool?

a. Identify open ports on a target system.
b. Identify the operating system that is running on a target system.
c. Identify the hosts available in a network.
d. Vulnerability available on a target system.

**Correct Answer**: a, b, c, d

**Detail Solution**: Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

The correct options are (a), (b), (c) and (d).

---

## QUESTION 6:

Which of the following NMAP commands are valid to run a nmap script “script_name.nse”?

a. nmap -- script=script_name.nse
b. nmap -- script script_name.nse

c. nmap -- script script_name

d. nmap script_name.nse

**Correct Answer**: a, b, c

**Detail Solution**: To run a nmap script "--script" option is used, script name can be assigned by given = symbol. However = symbol and writing the file name with extension (.nse) is optional.
The correct options are (a), (b) and (c).

---

## QUESTION 7:

Which of the following http scripts can be used to detect if a target system is running a webserver?

a. http-methos
b. http-brute
c. http-slowloris-check
d. ftp-anon

**Correct Answer**: a

**Detail Solution**: http-methos script is used to check if the host is running a web server on particular port. It can also identify if the supported methods (i.e. POST, GET etc). http-brute script is used for a dictionary attack on web server to get some valid credentials. http-slowloris-check script is used to detect a web server vulnerability for DoS attack. ftp-anon script is used to identify if the host is running ftp server or not, it can also identify if it provides anonymous login on ftp or not.

The correct option is (a).

---

## QUESTION 8:

Which of the following approaches can be used to create a secure hacking environment?

a. Use of proxy tools/servers
b. Using kali Linux in a live mode
c. Use of MAC changer tool
d. Use of firewalls
e. None of these

**Correct Answer**: a, b, c

**Detail Solution**: Using proxy servers, kali Linux/any other attacking OS in live mode and changing a MAC address frequently are some of the best options for a secure hacking environment. Firewall can save you from scanning, but will not provide any kind of security if you are attempting an attack to any system.

The correct options are (a), (b), and (c).

---

## QUESTION 9:

Assume that we want to connect to a target system (10.0.0.1) through ssh service, the username and password are “user” and “pwd” respectively. Which of the following commands can be used to create a ssh connection?

a. ssh 10.0.0.1 -l user
b. ssh 10.0.0.1 -l user -p pwd
c. ssh 10.0.0.1 user pwd
d. ssh user@10.0.0.1

**Correct Answer**: a, d

**Detail Solution**: To create a ssh connection, the ssh command is used. With this command username is provided by using -l option or can be combined with target IP address using @ symbol. Password is asked by target after validating username.

The correct options are (a), and (d).

---

## QUESTION 10:

Which of the following approaches can be used to enumerate all user available in a target system?

a. Use of nmap script smb-enum-user
b. Hydra tool
c. Crunch tool
d. Enum4linux

**Correct Answer**: a, d

**Detail Solution**: An nmap script smb-enum-user and enum4linux tools can be used to retrieve user information. Enum4linux tools can also enumerate password related information such as password policy. Hydra is used for password cracking, whereas crunch is used to create dictionary.

The correct options are (a) and (d).

---

## QUESTION 11:

Which of the following ports should be open on the target system to run a nmap script http-malware-host?

a. http
b. ssh
c. telnet
d. Dose not require any services to be running

**Correct Answer**: a

**Detail Solution**: The http-malware-host script works only if the target is hosting a web server and the http port is open.

The correct option is (a).

---

## QUESTION 12:

In an attack using the remote administrative tool, which part of the tool needs to be placed in target system?

a. Client
b. Server

**Correct Answer**: b

**Detail Solution**: In remote administrative tool attack, server part of the tool needs to be placed on the target system.

The correct option is (b).

---

## QUESTION 13:

Which of the following protocol(s) is/are not vulnerable to sniffing?

a. HTTP
b. Telnet
c. POP
d. HTTPS
e. SMTP

**Correct Answer**: d

**Detail Solution**: In HTTPS protocols packet transmission is done securely and in encrypted format; thus it is not vulnerable to sniffing attacks.

The correct option is (d).

---

## QUESTION 14:

The major loophole of ARP is that “a host can send unlimited number of ARP requests”, and this can be used for ARP spoofing / ARP poisoning.

a. True

b. False

**Correct Answer**: a

**Detail Solution**: In ARP protocol there is no limitations to send an ARP request, and this loophole is used to create ARP-based attack by sending multiple false ARP requests in network to flood ARP tables.

The correct option is (a).

---

## QUESTION 15:

Which of the following commands is used to see arp table in a system?

a. arp -a
b. arp -s
c. arp -i
d. arp -d

**Correct Answer**: a

**Detail Solution**: To access all information related to ARP, arp command is used, -a option is used to see all arp entries, -s option is used to create new arp entry, -i option is used to specify a particular network interface, -d option is used to delete an arp entry.

The correct option is (a).

---

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment- Week 6

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

15 parties want to exchange messages securely using a symmetric key encryption algorithm. The number of distinct key values required will be:

a. 30
b. 225
c. 210
d. 105

**Correct Answer: d**

**Detail Solution:** In symmetric encryption, every pair of communicating parties must have a separate key. For N parties, the number of keys will be ${}^{N}C_2$. For N = 15, ${}^{15}C_2 = 15 \times 14 / 2 = 105$.

The correct option is (d).

---

**QUESTION 2:**

200 parties want to exchange messages securely using some public key encryption technique like RSA. The number of distinct key values required will be _____

**Correct Answer: 400**

**Detail Solution:** In public-key or asymmetric encryption, every party is in possession of two keys, a public key and a private key. For N parties, the number of keys will be 2N. For N = 200, the number of distinct keys required will be 200 x 2 = 400.

---

**QUESTION 3:**

What are the effective key lengths used in DES and triple-DES symmetric key encryption algorithms in bits?

a. 56 and 168
b. 56 and 112

c. 56 and 56
d. 64 and 128
e. None of these

**Correct Answer: a**

**Detail Solution:** In the DES algorithm, the key size is 56 bits. In triple-DES, we have three sequential runs of the DES algorithm. Hence, in triple-DES, the effective key size will be $56 \times 3 = 168$ bits. Thus, the correct option is (a).

---

**QUESTION 4:**

On which difficult mathematical problem does the security of RSA algorithm depend on?

a. Discrete logarithm problem.
b. Testing whether a given number if prime or not.
c. Prime factorization problem.
d. The RSA threshold detection.
e. All of these.

**Correct Answer: c**

**Detail solution:** The security of the RSA algorithm depends on the complexity of factoring the product of two large prime numbers. The correct option is (c).

---

**QUESTION 5:**

Which of the following types of attack can the DoS attack be categorized into?

a. Interruption
b. Interception
c. Modification
d. Fabrication

**Correct Answer: a**

**Detail Solution:** In the denial-of-service (DoS) attack, the attacker makes a system/service inaccessible from legitimate users. This is a type of interruption attack.

The correct option is (a).

---

**QUESTION 6:**

Which of the following terms concern verifying the identity of the sender?

a. Encryption.
b. Authentication.
c. Decryption.
d. None of these.

**Correct Answer: b**

**Detail Solution:** Authentication refers to the process of verifying the identity of the sender of a message. Hence, the correct option is (b).

---

**QUESTION 7:**

Consider a mono-alphabetic cipher with the following key value:

(A B C D I J K L E F G H M N O P U V W X Q R S T Y Z)

What will be the encrypted form of the message “W I N D O W” ?

a. W E N D H W
b. S K N G H S
c. S E N D O S
d. None of these.

**Correct Answer: c**

**Detail Solution:** According to the specified key, the letter ‘W’ maps to ‘S’, ‘I’ maps to ‘E’, ‘N’ maps to ‘N’, ‘D’ maps to ‘D’, and ‘O’ maps to ‘O’. Hence the encrypted form of “WINDOW” will be “SENDOS”.

Hence, the correct option is (c).

---

**QUESTION 8:**

How many AES rounds are required for 128-bit key size?

a. 10
b. 11
c. 12
d. 14

**Correct Answer: a**

**Detail Solution:** 10 rounds are required in the AES algorithm for 128-bit key size.

The correct answer is (a).

---

**QUESTION 9:**

For encryption using public-key cryptography, we use the

a. Receiver's public key
b. Receiver's private key
c. Sender's public key
d. Sender's private key

**Correct Answer: a**

**Detail Solution:** If a sender A wants to carry out encryption on a message and send it to receiver B using public-key cryptography, A will encrypt the given message using B's public key, so that it can be correctly decrypted by the receiver B using B's private key.

Hence, the correct option is (a).

---

**QUESTION 10:**

Which of the following techniques is/are vulnerable to man-in-the-middle attack?

a. AES
b. RSA
c. Diffie-Hellman key exchange
d. None of these.

**Correct Answer: c**

**Detail Solution:** Diffie-Hellman key exchange protocol is vulnerable to the man-in-the-middle attack.

Hence, the correct option is (c).

---

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment- Week 7

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

Two messages M1 and M2 are fed to a hash function HASH to generate the hash values:

H1 = HASH (M1)

H2 = HASH (M2)

When do we say there is a collision?

a. H1 = H2.
b. M1 = M2.
c. H1 = HASH (H2).
d. None of these.

**Correct Answer: a**

**Detail Solution:** With respect to hashing, collision refers to the situation where more than one messages (here M1 and M2) map to the same hash value. The correct option is (a).

---

**QUESTION 2:**

What do you mean by first preimage resistance in the context of hash functions?

a. Except for few hash values H, it is difficult to find a message M such that HASH(M) = H.
b. Given a message M1, it is difficult to find another message M2 such that HASH(M1) = HASH(M2).
c. It is difficult to find two messages M1 and M2 such that HASH(M1) = HASH(M2).
d. None of these.

**Correct Answer: a**

**Detail Solution:** This follows from the definition of the desirable properties of a hash function. First preimage resistance refers to the condition that we are given a hash value H, and are

trying to find out some message M such that HASH(M) = H. This should be difficult to do. The correct option is (a).

---

**QUESTION 3:**

What kind of mapping does a hash function implement?

a. One-to-one mapping.
b. Many-to-one mapping.
c. One-to-many mapping.
d. Many-to-many mapping.

**Correct Answer: b**

**Detail Solution:** A hash function is one that maps a larger-size message to a smaller-size hash value. Several different messages may map to the same hash value, but the converse is not true. The correct option is (b).

---

**QUESTION 4:**

Which of the following is/are not hash functions?

a. MD5
b. Triple-DES
c. SHA-1
d. RSA.

**Correct Answer: b, d**

**Detail Solution:** MD5 and SHA-1 are examples of hash function, while Triple-DES is a symmetric key encryption algorithm, and RSA is a public key encryption algorithm. The correct options are (b) and (d).

---

**QUESTION 5:**

Which of the following algorithms are the slowest and the fastest?

Symmetric-key encryption, public-key encryption, hash function

a. Hash function, Symmetric-key encryption
b. Public-key encryption, Symmetric-key encryption
c. Symmetric-key encryption, Hash function

d. None of these.

**Correct Answer: d**

**Detail Solution:** Computation of hash function is the fastest, which computation of public-key encryption is the slowest. Symmetric-key encryption lies in between the two. Hence, the correct option is (d).

---

**QUESTION 6:**

What are the block size of DES algorithm and the hash digest size of MD5 algorithm?

a. 64 bits, 64 bits
b. 56 bits, 128 bits
c. 64 bits, 128 bits
d. 64 bits, 256 bits

**Correct Answer: c**

**Detail Solution:** In the DES algorithm, the block size is 64 bits and the key size is 56 bits. The hash digest size of the MD5 algorithm is 128 bits. The correct option is (c).

---

**QUESTION 7:**

On which cryptographic algorithm can the birthday attack be mounted?

a. Cryptographic hash function.
b. Symmetric-key cryptography.
c. Public-key cryptography.
d. Diffie-Hellman key exchange.
e. None of these.

**Correct Answer: a**

**Detail Solution:** Birthday attack utilizes some statistical properties to mount attacks on cryptographic hash functions. The correct option is (a).

---

**QUESTION 8:**

What kinds of algorithms are typically used in the computation of digital signature?

a. Cryptographic hash function.

b. Symmetric-key encryption.
c. Public-key encryption.
d. All of these

**Correct Answer: a, c**

**Detail Solution:** Digital signature is the electronic equivalent of pen-and-paper signature, and typically uses a combination of hashing and public-key cryptography. A hash function is first computed on the given message, and the hash value is encrypted using public-key cryptography, with the sender's private key. The correct options are (a) and (c).

---

**QUESTION 9:**

The SSL record protocol is responsible for

a. Data encryption
b. Data authentication
c. Non repudiation
d. All of these

**Correct Answer: a**

**Detail Solution:** The SSL Record protocol uses a combination of various cryptographic techniques to provide secure data transmission over a network. It ensures data encryption and also data integrity (using a hash function). However, it does not provide authentication service or non-repudiation guarantee. The correct option is (a).

---

**QUESTION 10:**

Which of the following security protocols work above the IP layer in the TCP/IP protocol stack?

a. IPSec
b. TLS
c. SSL
d. HTTPS

**Correct Answer: b, c, d**

**Detail Solution:** The TLS, SSL and HTTPS protocols work above the IP layer, whereas IPSec protocol makes the IP layer secure. The correct options are (b), (c) and (d).

---

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

# Course Name: ETHICAL HACKING

## Assignment- Week 8

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

Which of the following statements correctly represents the term steganography?

a. Encrypting information so that it will not be legible to an unauthorized person.
b. Hiding information within some cover media file.
c. Secure way of communicating without sharing any key.
d. None of these.

**Correct Answer: b**

**Detail Solution:** Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, etc.). The correct option is (b).

---

**QUESTION 2:**

Which of the following is/are not instances of behavioral biometrics?

a. Fingerprint
b. Signature
c. Gait
d. Iris scan
e. Retina scan

**Correct Answer: a, d, e**

**Detail Solution:** Behavioral biometrics refers to biometrics that relate to human behavior, like signature (hand and finger movement) and Gait (walking style). However, fingerprint, Iris scan and Retina scan are properties of the human body and not dependent on the behavior. Hence, the correct options are (a), (d) and (e).

---

**QUESTION 3:**

Consider a color image of size 2000 x 2000, where each pixel is stored in 24-bits (containing red, green and blue components as 8-bits each). How many bytes of information can be hidden in the image by using LSB steganography technique? *Assume that only the least significant bit in each 8-bit color component is modified*.

a. 12,000,000 bytes
b. 8,000,000 bytes
c. 7,500,000 bytes
d. None of these.

**Correct Answer: d**

**Detail Solution:** Each pixel consists of 24 bits or 3 bytes, and hence 3 bits of information can be stored in each pixel. The number of bits of hidden information that can be stored in the whole image will be:

2000 x 2000 x 3 bits = 2000 x 2000 x 3 / 8 bytes = 15, 00,000 bytes.

The correct answer is (d).

---

**QUESTION 4:**

Which of the following statements is/are true in biometric systems?

a. For authentication application, a user template is compared against all possible templates stored in the database.
b. For verification / identification application, a user template is compared against a specific single template stored in the database.
c. They can provide 100% accuracy in security applications.
d. None of these.

**Correct Answer: d**

**Detail Solution:** When biometric is used for authenticating a known person, his/her biometric template is compared against the corresponding template stored in the database.

However, for identifying a person whose id is not known, his/her biometric template has to be compared with all the templates stored in the database.

None of the biometric systems can provide 100% accuracy.

Thus, option (d) is true.

**QUESTION 5:**

What is denial-of-service attack?

a. An attack on a system whereby stored files get modified or deleted.
b. An attack that prevents legitimate users from accessing some service.
c. An attack that destroys the stored password information in a system.
d. None of these.

**Correct Answer: b**

**Detail Solution:** In a denial-of-service attack, some service running on a victim machine is rendered inaccessible from legitimate users of the service. The correct option is (b).

---

**QUESTION 6:**

How does a Smurf denial-of-service attack work?

a. A ping request is sent from the victim machine to a broadcast address.
b. The attacker sends a large number of ICMP ping messages to the victim machine.
c. It exploits a vulnerability in the TCP connection establishment process.
d. None of these.

**Correct Answer: a**

**Detail Solution:** In the Smurf DoS attack, the victim gains entry into the victim machine (or spoofs the IP address) and then sends a ping request to a broadcast address. A large number of ping response packets are received, which can overload the victim. The correct option is (a).

---

**QUESTION 7:**

Which of the following attacks rely on the accumulation of TCP half-open connections on the server?

a. Ping of death attack.
b. SYN flooding attack.
c. Smurf attack.
d. None of these.

**Correct Answer: b**

**Detail Solution:** The SYN flooding attack tries to exploit a weakness in the TCP connection establishment phase. The attacker floods the victim machine with a large number of TCP connection requests, each of which is left as half-open (i.e. the third packet in 3-way handshake is not sent). Each connection request will take up some resources on the victim machine (e.g. port number, buffer space, etc.), and ultimately genuine requests will not get processed.

The correct option is (b).

---

**QUESTION 8:**

Which of the following is/are true for Botnet?

a. A large number of Botnets are often used to attack a victim machine.
b. It is a malicious software that spreads from one machine to another.
c. It can be used to mount distributed denial-of-service attack.
d. All of these.

**Correct Answer: a, c**

**Detail Solution:** Many of the network-based attacks (DoS and DDoS in particular) are based on so-called Botnets. A Botnet refers to a host connected to the Internet that is under the control of the attacker. The Botnet host runs a number of "bots" that are repetitive code segments with some malicious intent, typically used to mount an attack. It does not spread from one machine to another.

The correct options are (a) and (c).

---

**QUESTION 9:**

What is meant by recursive name resolution?

a. A host may have to send multiple DNS requests to several DNS servers.
b. A host sends a single DNS request to its next higher-level DNS server.
c. Name resolution happens recursively within the host itself.
d. All of these.

**Correct Answer: b**

**Detail Solution:** The DNS server receives a DNS request from a host containing a domain name, and it returns the corresponding IP address. In iterative name resolution, in response to a DNS request, the DNS server sends back a response specifying the next DNS server to send the

query. In this way, the host may have to send a number of DNS requests before it gets resolved. In recursive name resolution, the host sends a DNS request to the next higher level DNS server. The DNS server in turn recursively forwards the request to its next higher-level DNS server, and so on, until the request gets resolved. The final reply gets back to the host. Here, the host sends a single DNS request.

Thus, option (b) is true.

---

**QUESTION 10:**

How does PGP provide security in email transmission?

a. It provides authentication.
b. It provides non-repudiation.
c. It ensures availability.
d. All of these.

**Correct Answer: a**

**Detail Solution:** PGP provides a set of services for secure email transmission. It provides services like authentication and confidentiality, using a combination of hash functions and encryption techniques. However, it does not address availability or non-repudiation issues. The correct option is (a).

---

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

# Course Name: ETHICAL HACKING

## Assignment Solution- Week 9

### TYPE OF QUESTION: MCQ/MSQ/SA

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

---

**QUESTION 1:**

Why do packet sniffers require the network interface card (NIC) to be put in promiscuous mode?

a. So that broadcast packets can be sent to the victim machine.
b. So that all packets crossing the NIC can be read.
c. So that headers of encrypted packets can be deciphered.
d. None of these.

**Correct Answer: b**

**Detail Solution:** In the promiscuous mode, a packet sniffer can read all traffic on the network segment to which the NIC is connected (irrespective of sender and receiver). The correct option is (b).

---

**QUESTION 2:**

Which of the following measures can prevent packet sniffing on a network segment?

a. Restrict physical access to the network by unauthorized persons.
b. Install the latest version of TCP protocol that does not contain vulnerabilities.
c. Use encryption to protect confidential information.
d. All of these.

**Correct Answer: a, c**

**Detail Solution:** To run the packet sniffer, the adversary has to first gain physical access to one of the machines in the network; restricting physical access can prevent this. Also, if the packet payload is encrypted, even after sniffing the contents cannot be decoded. Packet sniffing does not depend on the version of the TCP protocol that is being used. The correct options are (a) and (c).

---

**QUESTION 3:**

How can NMAP detect whether network sniffing is probably going on in a network?

a. By sending a NMAP ping request to all the machines on the network.
b. By conducting TCP stealth scan on all the machines in the network.
c. By using a script that checks whether any of the machines has the network card configured in the promiscuous mode.
d. None of these.

**Correct Answer: c**

**Detail Solution:** Using the following NMAP command, we can find out whether any of the network cards on the network is configured in the promiscuous mode. (It is done by broadcasting fake ARP packets)

```
nmap –script=sniffer-detect <IP addresses to check>
```

The correct option is (c).

---

**QUESTION 4:**

Which of the following features are present in Ettercap?

a. IP-based and MAC-based filtering.
b. Character injection.
c. Packet filtering and dropping.
d. SQL injection.
e. All of these.

**Correct Answer: a, b, c**

**Detail Solution:** The Ettercap tool can carry out IP-based filtering, MAC-based filtering, character injection in a packet, packet filtering & dropping. However, it cannot be used to mount SQL injection attacks. The correct options are (a), (b) and (c).

---

**QUESTION 5:**

Which of the following can be used for computer-based social engineering attack?

a. Tailgating.
b. Sending out chain letter emails.
c. An illegitimate email falsely claiming to be from a legitimate site.
d. Reverse social engineering.

**Correct Answer: b, c**

**Detail Solution:** Tailgating and reverse social engineering are used for human-based social engineering attacks. Chain letter and phishing, as mentioned in (b) and (c), are example of computer-based social engineering attacks. The correct options are (b) and (c).

---

**QUESTION 6:**

Which of the following tools can be used to put the NIC in promiscuous mode?

a. macchanger
b. dnsenum
c. slowloris
d. arpspoof

**Correct Answer: d**

**Detail Solution:** macchanger tool is used for assigning random mac address, dnsenum is used for enumerating dns server, and Slowloris is used for mounting DoS attack. Using arpspoof we can poison the arp tables and it is used to put the NIC of the system in promiscuous mode.

The correct options is (d).

---

**QUESTION 7:**

Which of the following protocols are vulnerable to sniffing attack?

a. HTTP
b. FTP
c. HTTPS
d. SSL

**Correct Answer: a, b**

**Detail Solution:** HTTPS and SSL exchange data in secure channel, HTTP and FTP protocol exchanges data in plain text (unsecured form), thus it is vulnerable to sniffing attack.

The correct options are (a) and (b).

---

**QUESTION 8:**

How does Slowloris work?

a. It sends a single large packet to victim system.

b. It sends multiple HTTP requests to the victim system but never completes the request.
c. It mounts MAC attack on target system.
d. It turns on NIC of the system in promiscuous mode.

**Correct Answer: b**

**Detail Solution:** It sends multiple HTTP packets to connect with the victim system, but never completes resulting DoS for legitimate users.

The correct option is (b).

---

**QUESTION 9:**

Which of the following is/are example(s) of bandwidth flood?

a. ICMP flood
b. SYN flood
c. MAC Flood

**Correct Answer: a, b, c**

**Detail Solution:** In ICMP/MAC flood attack large number of ICMP/ARP packets are sent to victim. And once the ICMP/ARP tables are filled the system either act as unexpected nature (i.e. switch will start working as hub) or stops responding to legitimate user.

Similarly limited numbers of SYN requests can be handled by any system, and each SYN request must be open for 75 second so if an attacker tries sending large number of SYN packets then it causes DoS.

The correct options are (a), (b) and (c).

---

**QUESTION 10:**

For mounting DoS attack using hping3 tool what option can be used as an alternative of –i u10000?

a. --count
b. --fast
c. --faster
d. --flood

**Correct Answer: b**

**Detail Solution:** We use hping tool –I u10000 alias for sending 10 packets for a second, which is the same as using option –fast.

The correct option is (b).

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