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 point(s) is/are **true** for an ethical hacker?

a. An ethical hacker intends to gain unauthorized access to a resource for financial gain or personal recognition.
b. An ethical hacker defaces websites or crash backend servers for fun, reputation damage or to cause financial loss.
c. An ethical hacker is not concerned with improving the organization's security posture.
d. None of these.

Correct Answer: d

Detail Solution: Ethical hackers use their knowledge to secure and improve the technology of organizations. An ethical hacker reports the identified vulnerabilities to the organization. Malicious hackers intend to gain unauthorized access to a resource for financial gain or personal recognition. Some malicious hackers deface websites or crash backend servers for fun, reputation damage, or to cause financial loss. The methods used and vulnerabilities found remain unreported. They are concerned with improving the organization's security posture. Thus all the points given are false for an ethical hacker.

Thus the correct option is (d).

QUESTION 2:

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

a. In the black box model, the tester has complete information about the network.
b. In the white box model, the tester does not have any information about the network.
c. In the gray box model, the tester has partial information about the network.
d. None of these.

Correct Answer: 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.

Thus the correct option is (c).

QUESTION 3:

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

a. A communication link can be shared by more than one connection.
b. A communication link is dedicated to a connection and cannot be shared with other connections.
c. It is efficient for bursty traffic.
d. The packet transfer delay between a pair of nodes may depend on the prevailing network traffic.

Correct Answer: b

Detail Solution: 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. It is efficient for high bandwidth traffic like data streaming.

Thus the correct option is (b).

QUESTION 4:

Which of the following statement(s) is/are **true** for datagram-based packet transfer approach?

a. It is a connection-less packet switching approach, where no route is established priori to transfer of packets.
b. In this approach, each packet is transmitted as an independent entity.
c. In this approach each intermediate node can perform dynamic routing.
d. In this approach all the packets reach in order to the destination.

Correct Answer: a, b, c

Detail Solution: Datagram approach is a connection-less packet switching approach where no route is established before packet transmission starts. In this approach each packet is transmitted as an independent entity containing source and destination addresses. Thus it is not necessary to follow same path for all packets and thus the packets can be delivered out of order. For forwarding the packet to next node, every node maintains a routing table that is updated dynamically to take routing decision.

Thus correct options are (a), (b) and (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 uniquely identifies a running application on a specific host in the network.
d. It indicates how many hardware ports are there in the computer system.
e. None of these.

Correct Answer: c

Detail Solution: Port number uniquely identifies a running application on a specified host in the network.

Thus the correct option is (c).

QUESTION 6:

Which of the following is **not** a valid port numbers in TCP/IP?

a. 21
b. 80
c. 443
d. 8080
e. 80800

Correct Answer: e

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 invalid port number is 80800 (option e).

QUESTION 7:

Which of the following functionality does Address Resolution Protocol (ARP) perform?

a. Map IP addresses to hardware (MAC) addresses.
b. Map hardware addresses (MAC) to IP addresses.
c. Performs error control and correction.
d. Breaks the packet into smaller packets, if required.

Correct Answer: a

Detail Solution: ARP is responsible for mapping IP addresses to MAC addresses.

Thus the correct option is (a).

QUESTION 8:

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

a. IP provides connectionless, unreliable delivery systems for packets.
b. UDP provides connectionless, unreliable delivery systems for packets
c. TCP provides connectionless, unreliable delivery systems for packets.
d. None of these.

Correct Answer: c

Detail Solution: IP and UDP provide connectionless, unreliable delivery systems for packets. However TCP provides a connection-oriented reliable service.

Thus the correct option is (c).

QUESTION 9:

If the IP header is 96 bits long, what will be the value (in decimal) of the "HLEN" field _____?

Correct Answer: 3

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 = 96 bits = 3 x 32 bits. Hence, HLEN will contain 0011, which is the binary equivalent of the number 3.

Thus the correct answer will be 3.

QUESTION 10:

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.

**********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:

Why there is a need for fragmentation of IP packets?

a. Fragmentation is necessary because every network has a unique limit for the maximum size of datagrams that it can process.
b. Fragmentation is necessary for faster data transfer.
c. Fragmentation is necessary for error-recovery and flow control.
d. All of these.

Correct Answer: a

Detail Solution: IP fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process, which is known as maximum transmission unit (MTU). In fragmentation, the packets are divided into smaller pieces and each piece is considered as separate IP packet. This is typically done by the routers in the network layer (or layer-3 switches).

Thus the correct option is (a).

QUESTION 2:

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

a. In transparent fragmentation the subsequent networks are aware that the fragmentation had occurred.
b. In transparent fragmentation, it is required to route all packet to the same exit router in a network.
c. In non-transparent fragmentation, each fragment is treated as an independent packet.
d. In non-transparent fragmentation, an exit router reassembles all fragmented packets.

Correct Answer: b, c

Detail Solution: In transparent fragmentation, all packets are routed through an exit router that assembles the fragmented packets. In this approach the subsequent network(s) have no information about fragmentation. Whereas in non-transparent fragmentation the packets can be transmitted through multiple routers as each packet is treated as independent packet and the reassembly is done by the destination host system.

Thus the true options are (b) and (c).

QUESTION 3:

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

a. Prevents the fragmentation from taking place.
b. The packet will be fragmented by the next router.
c. The packet represents a fragment of a larger packet.
d. None of these.

Correct Answer: c

Detail Solution: When the More (M) flag in a packet is 1, this indicates that the original packet has definitely been fragmented and there are more fragments following.

Thus the true option is (c).

QUESTION 4:

Which of the following statement(s) is/are **false** for IP address?

a. IP address is 32-bit quantity.
b. IP address is typically expressed as dotted decimal notation where dots are used to separate each of the four octets of the address.
c. IP address consists of three logical parts: network number, host number and port number.
d. None of these.

Correct Answer: c

Detail Solution: IP address is 32-bit quantity, it is expressed as dotted decimal notation where dots are used to separate each of the four octets of the address. IP address consist of two logical parts: network number and host number, while routing a packet to the destination network, only

the network number is looked at whereas for uniquely identification of the system inside a network host number is used which is managed by local network administrator.

Thus the correct option is (c).

QUESTION 5:

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 is Class B, and the second one is Class A address.

Hence, the correct option is (c).

QUESTION 6:

Which of the following IP addresses represent broadcast address?

a. 144.15.255.255
b. 144.16.0.255
c. 202.0.255.250
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 7:

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

Correct Answer: 254

Detail Solution: For a class C network, 8 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 $2^8 - 2 = 254$.

QUESTION 8:

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).

QUESTION 9:

In the TCP header field, what do SYN=1 and ACK=0 represent?

a. Connection request message.
b. Connection confirmation message.
c. Reject connection request.
d. Reset connection request.

Correct Answer: a

Detail Solution: In the TCP header, SYN=1 and ACK=0 represents connection request, whereas SYN=1 and ACK=1 represents connection confirmation. RST is used to reset/reject connection.

Thus the correct option is (a)

QUESTION 10:

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: d

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

```
144.16.75.105  =  10010000 00010000 01001011 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 01000000 00000000 = 144.16.64.0
```

******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:

Consider the following statements:

(i) In connection-oriented approach, network layer first makes a connection.

(ii) IP protocol uses connection-oriented routing.

a. Only (i) is true
b. Only (ii) is true
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: a

Detail Solution: In connection-oriented approach, network layer first makes a connection and then all packets are delivered as per the connection. In connection-less protocol, network layer treats each packets independently. IP protocol uses connection-less approach for packet delivery.

Thus option (a) is correct.

QUESTION 2:

Which of the following is/are **true** for default route?

a. Default route is used when no specific address for next hop is available.
b. In routing table default route is specified by an address 0.0.0.0.
c. In routing table default route is specified by an address 255.255.255.255.
d. In routing table default route is specified by an address 127.0.0.1.
e. None of these.

Correct Answer: a, b

Detail Solution: Default route, also known as the gateway of last resort, is used in forwarding packets whose destination address does not match any route in the routing table. In IPv4 the CIDR notation for a default route is 0.0.0.0/0.

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

QUESTION 3:

Which of the following is/are **true** for static routing?

a. In static routing routes are user defined.
b. In static routing, routing table updates periodically depending on the network condition.
c. Static routing is easy to configure.
d. None of these.

Correct Answer: a

Detail Solution: In static routing routes are defined manually and the routing table does not change until the network administrator changes manually or modify them manually. Also if any network change occurs, then the complete table needs to be modified.

Thus the true option is (a).

QUESTION 4:

Which of the following routing flags indicates that the router is up and running?

a. U
b. G
c. H
d. D
e. M

Correct Answer: a

Detail Solution: U flag indicates if the router is up and running.

The correct option is (a).

QUESTION 5:

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 6:

Which of the following statement(s) is/are **false** for Routing Information Protocol (RIP)?

a. RIP is an example of interior routing protocol.
b. RIP maintains timers to detect failed links.
c. RIP converges faster for large networks.
d. RIP consumes high bandwidth to update routes.
e. None of these.

Correct Answer: c

Detail Solution: RIP shows slow convergence for larger network, because to confirm or detect any failed link it requires to send larger number of packets as compare to other routing protocols.

Thus correct option is (c).

QUESTION 7:

Which of the following is/are **false** for Border Gateway Protocol (BGP)?

a. BGP allows routers belonging to different autonomous systems to exchange routing information.
b. BGP uses TCP connection to send routing messages.
c. BGP can also be used by routers within the same autonomous systems.
d. BGP sends keepalive messages periodically to ensure that the connection between the BGP peers is alive.

e. None of these.

Correct Answer: e

Detail Solution: BGP is used for exchanging routing information by the routers belongs to different autonomous systems. However it can also be used to exchange information by routers within same AS. BGP sends routing information through TCP connection. Two BGP routers exchange information on a connection are called peers, to know if the peer is alive or not. BGP sends keepalive message periodically to its peer.

Thus the correct option is (e).

QUESTION 8:

If a packet is to be delivered to a specific host 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: a

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.

Thus, the correct option is (a).

QUESTION 9:

Which of the following is **not true** for IPv6?

a. It uses 32-bit IP addresses.
b. IPv6 address does not have any defined classes.
c. It uses 128-bit IP addresses.
d. None of these.

Correct Answer: a

Detail Solution: IPv6 uses 128-bit IP addresses, and provides a large address space. Unlike IPv4 it does not have any defined classes.

Thus the correct option is (a).

QUESTION 10:

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).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Ethical Hacking

Assignment- Week 4

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1:

Which of the following statement(s) is/are **true** for NAT networking mode?

a. In NAT mode, the virtual machines cannot access each other.
b. NAT mode does not allow access of internet to the installed virtual machines.
c. In NAT mode, the hypervisor allocate same IP address to all virtual machines.
d. All of these.

Correct Answer: a, c

Detailed Solution:

By default, virtual box uses NAT mode. In this mode internet access is allowed; however, each system gets the same IP, and thus the virtual machines cannot access each other in this mode.

Thus the correct options are (a) and (c).

QUESTION 2:

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 a chance of detection.
d. There is no chance of detection.

Correct Answer: a, d

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, e.g., web search. As the attacker and victim does not communicate directly, there is no a chance of detection.

Thus the true options are (a) and (d).

QUESTION 3:

Which of the following can be used for active reconnaissance.

a. Whois
b. Archive.org
c. NMAP
d. Nessus
e. Metasploit
f. Hydra

Correct Answer: c, d, e

Detailed Solution: Whois and archive are used for passive reconnaissance. NMAP, Nessus and Metasploit are used in active reconnaissance as they directly communicate with the target system. Hydra is a tool used for password cracking.

The correct options are (c), (d) and (e).

QUESTION 4:

Which of the following information **cannot** be retrieved using active reconnaissance?

a. Live host in a network.
b. Open ports.
c. Services running in the systems.
d. Operating system of the target system.
e. Vulnerabilities of target machine/application.
f. None of these.

Correct Answer: f

Detailed Solution: In active reconnaissance scanning tool performs major role, it can be used for identification of live host, active ports, services, operating system and vulnerabilities of the target system.

The correct option is (f).

QUESTION 5:

Which of the following tools **cannot** be used for DNS enumeration?

a. host
b. dnsenum
c. dig
d. None of these

Correct Answer: d

Detailed Solution: For DNS enumeration various tools can be used such as host, dnsenum, dig, nslookup, nmap, dnsrecon, etc.

The correct option is (d).

QUESTION 6:

What is the main objective of host discovery?

a. Identification of live hosts.
b. Identification of services running in the target system.
c. Identification of version of the services running in the target system.
d. Identification of the operating system of the target systems.
e. Identification of open ports.

Correct Answer: a

Detailed Solution: The main objective of host discovery is to identify the live hosts in the network or network infrastructure.

The correct option is (a).

QUESTION 7:

Which of the following options is used to trace the details of the sent/received packets?

a. --packet-trace
b. --reason
c. --disable-arp-ping
d. None of these

Correct Answer: a

Detailed Solution: To get the details of the packets used for scanning, --packet-trace option can be used. – reason option is used to get the reason of the report (why the port/system is up/down). – disable-arp-ping is used to disable arp table check.

The correct option is (a).

QUESTION 8:

Which of the following options can be used to perform ICMP ECHO sweep?

a. –PE
b. –PP
c. –PM
d. –PU

Correct Answer: a

Detailed Solution: In ICMP ECHO 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. To perform ICMP ECHO sweep scan –PE option is used.

Thus the correct option is (a).

QUESTION 9:

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

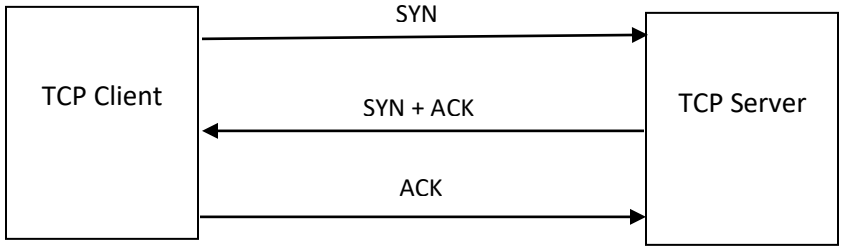
Detailed Solution: TCP connection establishment involves a 3-way handshake.

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.

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 10:

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 or not.
b. It completes the 3-way handshake in TCP connection establishment, and decides whether the port is open.
c. It does not use 3-way handshake.
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 11:

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 12:

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.

The correct option is (a).

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:

If we does not want to carry out port scanning then which of the following options can be used with NMAP?

a. -F
b. -p-
c. -Pn
d. -sn
e. We cannot disable port scanning.

Correct Answer: d

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 (d).

QUESTION 15:

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).

********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
e. Crunch

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. Hypervisor is a software tool used for virtualization. Hydra and Crunch are used for performing password attack.

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

QUESTION 2:

NMAP scripts can be used for:

a. Vulnerability scanning
b. Backdoor detection.
c. Port detection.
d. Password attack.
e. None of these.

Correct Answer: a, b, c, d

Detail Solution: The NMAP scripts can be useful for automated scanning. NMAP scripts can be used for vulnerability detection, backdoor detection, port detection, performing password attacks etc.

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

QUESTION 3:

Which of the following NMAP scripts is used to identify the OS of a target system?

a. smb-os-brute
b. smb-os-discovery
c. http-os-check
d. None of these.

Correct Answer: b

Detail Solution: smb-os-discovery is used to identify the OS of the target system; there is no script such as smo-os-brute, http-os-check.

Thus the correct option is (b).

QUESTION 4:

Which of the following scripts can be used to detect if a target system is vulnerable to DoS attack?

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

Correct Answer: d

Detail Solution: http-methos script is used to check if the host is running a web server on particular port. It can also identify 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. There is no script named as http-dos-check.

The correct option is (d).

QUESTION 5:

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 –p pwd
b. ssh 10.0.0.1 -l pwd -p user
c. ssh 10.0.0.1 user pwd
d. None of these

Correct Answer: 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. None of the commands are correct.

Thus the correct option is (d).

QUESTION 6:

The necessary parameters required to generate word list using crunch tool is:

a. Minimum length of the word list.
b. Maximum length of the word list.
c. File name where the word list will be stored.
d. No parameters are required to generate a word list.

Correct Answer: a, b

Detail Solution: To generate a word list using crunch, the necessary parameters which needs to be provided are minimum and maximum length of the word list. All other parameters are optional.

Thus the correct options are (a) and (b).

QUESTION 7:

Which of the following tools can be used to perform password attack?

a. Hydra
b. Archive.org
c. Netcraft
d. Whois
e. None of these.

Correct Answer: a

Detail Solution: To perform password attack we can use Hydra tool.

Thus the correct option is (a).

QUESTION 8:

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. Triangular privilege escalation.
e. 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/triangular privilege escalation.

Thus the correct option is (a).

QUESTION 9:

Which of the following approaches can be used to extract information about all users 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 10:

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 11:

To upload any file in the target system which is connected through FTP connection which of the following command can be used?

a. put
b. get
c. upload
d. download

Correct Answer: a

Detail Solution: To upload any file we use the "put" command.

The correct option is (a).

QUESTION 12:

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 13:

How a malware can get inside into a system?

a. Removable devices
b. Attachments
c. Fake Programs
d. Untrusted sites and freeware software.

Correct Answer: a, b, c, d

Detail Solution: Malware can get inside the system through all the given approaches.

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 all arp entries 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*******

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:

Which of the following is not an example of active security attack?

a. Masquerade
b. Replay
c. Traffic analysis
d. Modification
e. Denial of Service.

Correct Answer: c

Detail Solution: Analyzing the network traffic refers to passive attack. Masquerade, replay, modification, denial of service are active attacks.

Thus the correct option is (c).

QUESTION 2:

Consider the following statements:

(i) In symmetric key cryptography, single shared key is used by sender and receiver.
(ii) In Asymmetric key cryptography, separate keys are used by sender and receiver.

a. Only (i) is true
b. Only (ii) is true
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: In symmetric key (private key) cryptography, a single key is shared and used by sender and receiver, whereas in public key cryptography separate keys are used by sender and receiver.

Thus correct option is (c).

QUESTION 3:

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

Correct Answer: 105

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, ${}^{15}C_2 = 15 \times 14 / 2 = 105$.

QUESTION 4:

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 5:

How many AES rounds are required for 192-bit key size?

a. 10
b. 11

c. 12
d. 14

Correct Answer: c

Detail Solution: 12 rounds are required in the AES algorithm for 192-bit key size.

The correct answer is (c).

QUESTION 6:

What is the key length in data encryption standard (DES)?

a. 56
b. 64
c. 128
d. 192

Correct Answer: a

Detail Solution: The DES encryption algorithm is a "block cipher" that encrypts information in blocks of 64 bits (8 bytes). Using a 56-bit key, DES encrypts each block in 16 identical rounds.

The correct answer is (a).

QUESTION 7:

100 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: 200

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 = 100, the number of distinct keys required will be 100 x 2 = 200.

QUESTION 8:

In Digital signature sender signs a message with its:

a. Private key
b. Public key

Correct Answer: a

Detail Solution: For digital signature or authentication sender signs a message with its private key that is authenticated by the corresponding public key.

Thus the correct option is (a).

QUESTION 9:

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 10:

Which of the following statement(s) is/are **true** for Diffie-Hellman Key Exchange algorithm?

a. It allows group of users to agree on secret key over insecure channel.
b. The security of the algorithm depends on prime factorization problem.
c. The algorithm is vulnerable to man-in-the-middle attack.
d. It does not require any prior communication between sender and receiver.
e. All of these.

Correct Answer: a, c, d

Detail solution: D-H algorithm is mainly used for key exchange between users over an insecure channel; it does not require any prior communication between sender and receiver for key exchange. As the communication is done over insecure channel it is vulnerable to man-in-the-middle attack. The complexity of the algorithm depends on that of cracking the discrete logarithm problem.

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

**********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:

Which of the following is/are **true** for Unkeyed hash function (Modification Detection Code)?

a. Unkeyed hash function is used to preserve integrity of message.

b. Unkeyed hash function is used to authenticate source of message.

c. Unkeyed hash function produces an output that depends only on the input data.

d. None of these.

Correct Answer: a, c

Detail Solution: Unkeyed hash function takes an input of variable length and converts it to a fixed-length output. It does not use any key, and thus the output only depends on the input data. Unkeyed hash function is used to preserve data integrity. It is impossible to figure out the sender of the message when we use Unkeyed hash function.

Thus the correct options are (a) and (c).

QUESTION 2:

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 3:

Which of the following corresponds to second preimage resistance in the context of hash functions?

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

Correct Answer: b

Detail Solution: When we use hash function then it is expected that it should be computationally infeasible to identify the input data; for this preimage resistance and collison rules are used.

The first preimage resistance is defined as: Except for few hash values H, it should be difficult to find a message M1 such that HASH(M1) = H. This means that for all pre-specified outputs, it should be computationally infeasible to find any input which hashes to that output.

The second preimage resistance is defined as: Given a message M1, it should be difficult to find another message M2 such that HASH(M1)=HASH(M2), which means it should be computationally infeasible to find any second input which has the same output as any specified input.

Collison resistance is defined as: It should be difficult to find two messages M1 and M2 such that HASH(M1)=HASH(M2). This means it should be difficult to find two messages with same hash values.

The properties of second preimage resistance and collision resistance may seem similar but the difference is that in the case of second preimage resistance, the attacker is given a message to

start with, but for collision resistance no message is given; it is simply up to the attacker to find any two messages with same hash values.

The correct option is (b).

QUESTION 4:

What is the message digest length of MD5 and SHA-1 hash functions?

a. 32-bit, 64-bit.
b. 64-bit, 128-bit.
c. 128-bit, 160-bit.
d. 128-bit, 256-bit.
e. None of these.

Correct Answer: c

Detail Solution: MD5 and SHA-1 hash function results in 128-bit and 160-bit hash values that is often termed as message digest.

The correct option is (c).

QUESTION 5:

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 6:

Hash functions are faster than symmetric and public key encryption?

a. True
b. False

Correct Answer: a

Detail Solution: Computation of hash function is the fastest. Computation of public-key encryption is the slowest. Symmetric-key encryption lies in between the two.

Hence, the correct option is (a).

QUESTION 7:

Which of the following is/are **false** for digital signature?

a. Digital signature is legally equivalent to hand-written signature.
b. In digital signature, signer uses his public key to sign.
c. Anybody having access to the signer's public key can verify the signature.
d. None of these.

Correct Answer: b

Detail Solution: Digital signature is an example of authentication where the signer uses his private key to sign any document, a receiver or anybody having the access of public key of the signer can identify the signer, digital signature is equivalent to hand written signature.

The correct option is (b).

QUESTION 8:

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

a. Secure Socket Layer (SSL) provides security to the data transferred between web browser and server.
b. SSL can be used for any network service running over TCP/IP.
c. SSL Handshake Protocol provides mutual authentication.
d. None of these.

Correct Answer: a, b, c

Detail Solution: SSL is used to provide secure channel for data transfer. It uses TCP to provide reliable end-to-end secure service and can be used for any network service running over TCP/IP. SSL is responsible for data security and integrity; it can also perform some other functionalities such as fragmentation and encryption. SSL Handshake Protocol is used to initial session between server and client and provides mutual authentication.

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

QUESTION 9:

Which of the following statement(s) is/are **true** for SSL Alert Protocol?

a. If the first byte is 1 then it indicates that this alert has no impact on the connection between sender and receiver.
b. If the fist byte is 1 then the SSL connection is terminated.
c. If the first byte is 2 then it indicates that this alert has no impact on the connection between sender and receiver.
d. If the first byte is 2 then the SSL connection is terminated.

Correct Answer: a, d

Detail Solution: SSL Alert protocol is used to send session messages associated with data exchange and functioning of the protocol. Each SSL alert message consists of two bytes. The first byte can be either 1 or 2. The value 1 indicates warning such as bad certificate, no certificate, certificate expired, unsupported certificate etc. This alert does not have any impact on the session. The value 2 indicates the fatal error such as handshake failure, incorrect MAC etc. which leads to connection termination. The second byte describes the error.

Thus the correct options are (a) and (d).

QUESTION 10:

Consider the following statements:

(i) SSL is designed to establish secure connection between two hosts.

(ii) s-HTTP is designed to send individual messages securely.

a. Only (i) is true
b. Only (ii) is true

c. Both (i) and (ii) are true
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: Secure HTTP is an extension of HTTP protocol that is used to send data securely over the web. The main difference between SSL and s-HTTP is that SSL is designed to establish a secure connection between two hosts whereas s-HTTP is designed to send individual messages securely.

The correct option is (c).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

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:

Consider the following statements:
(i) Steganography refers to a set of methods to hide some secrete information in an audio/image/executable files.
(ii) Steganography and digital watermarking shares same operational and functional behaviors.

a. Only (i) is true
b. Only (ii) is true
c. Both (i) and (ii) are true
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, executable, etc.). Digital watermarking embeds copyright, ownership, license and similar information in a medium such as audio, video, image etc. Digital watermarking is different from steganography only in the intent of hiding. They share same operational and functional behavior.

The correct option is (c).

QUESTION 2:

Consider a gray-level image of size 2000 x 2000, where each pixel is stored in 24-bits (containing red, green, and blue components as 8-bit 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).*

Correct Answer: 1500000

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.

QUESTION 3:

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

a. Biometrics refers to an automated method for hiding information in a media like audio, video, image etc.
b. Biometrics refers to embedding copyright, ownership, license and similar information in a medium such as audio, video, image etc.
c. Biometrics refers to an automated method for recognizing individuals based on measurable biological and behavioral characteristics.
d. None of these.

Correct Answer: c

Detail Solution: Hiding information is referred to as steganography, hiding information such as copyright is known as digital watermarking. Biometrics refers to an automated method for recognizing individuals based on measurable biological and behavioral characteristics.

The correct option is (c).

QUESTION 4:

Which of the following is/are example(s) of behaviour biometric?

a. Retina scan
b. Fingerprint recognition
c. Facial recognition
d. None of these

Correct Answer: d

Detail Solution: Physical biometrics refers to physiological features on the human body such as a fingerprint, retina scan whereas behavioral biometrics analyzes parameters such as keystroke pattern, typing speed, mouse movement, signature styles etc.

The correct option is (d).

QUESTION 5:

Which of the following statement(s) 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 application, a user template is compared against a specific single template stored in the database.
c. Biometric systems 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 6:

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 7:

In which of the following denial-of-service attacks, the attacker attempts to crash/freeze target computer/service by sending oversized packet in simple ping command?

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

Correct Answer: c

Detail Solution: In the ping-of-death attack, attacker uses larger than maximum packet size (65536) ping packets that are broken into smaller segments and resembled at receiver end. Systems that are unable to handle such abnormalities either crash or reboot.

The correct option is (c).

QUESTION 8:

Which of the following statement(s) is/are true for HTTP Flood attack?

a. It is a type of Distributed-Denial-of-Service (DDoS) attack.
b. It overwhelms a target server by accumulating large number of TCP half-open connections.
c. It overwhelms a target server using oversized ping packets.
d. It overwhelms a target server with HTTP request.
e. None of these.

Correct Answer: a, d

Detail Solution: HTTP Flood attack is a type DDoS attack which is designed to overwhelm the target server with HTTP requests. Once the target is saturated with HTTP requests, it does not respond to HTTP request from legitimate users.

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

QUESTION 9:

Which of the following approach can be used to mitigate HTTP flood attack?

a. Use captcha test.
b. Use JavaScript computational challenge.
c. Use web application firewall.
d. Block ping requests.
e. Block TCP connections.
f. None of these.

Correct Answer: a, b, c

Detail Solution: To protect web server from HTTP flood attack a simple method can be giving challenge to the requesting machine in order to test whether it is a bot or a legitimate user. For this we can use captcha test or simple JavaScript computational challenge.

The other way to mitigate HTTP flood attack is to use web application firewall that can identify an authentic source of traffic and selectively block all malicious traffic.

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

QUESTION 10:

Which of the following is true for 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 the correct option is (b).

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

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:

In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read all traffic on the network segment to which the adapter is connected.

a. True
b. False

Correct Answer: a

Detail Solution: In computer networking, promiscuous mode is a mode of operation, as well as a security, monitoring and administration technique which is mostly used for network analyzer tools such as Wireshark and burpsuit. In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read in its entirety each network packet that arrives.

Thus the correct option is (a).

QUESTION 2:

Which of the following commands can be used to put the NIC of a machine to promiscuous mode? (Assumption: Machine IP - 192.168.43.48, IP of default gateway - 192.168.43.141, the machine is connected with eth0 interface).

a. arpspoof 192.168.43.48
b. arpspoof 192.168.43.141
c. arpspoof –i eth0 192.168.43.48
d. arpspoof –i eth0 192.168.43.141

Correct Answer: d

Detail Solution: To put any machine (say M) into promiscuous mode we need to send fake ARP messages to all devices stating that the MAC address of default gateway is changed to the MAC address of the machine M.

To achieve this, arpspoof tool is used, and the command used for the same is arpspoof –i 192.168.43.141.

The correct option is (d).

QUESTION 3:

In Wireshark, to filter all the packets used by an IP address 23.36.4.106, which of the following filter option/command can be used?

a. 23.36.4.106
b. ip == 23.36.4.106
c. ip.addr == 23.36.4.106
d. ip.address = 23.36.4.106
e. None of these.

Correct Answer: c

Detail Solution: To filter all packets "ip.addr ==" option is used along with the IP address.

The correct option is (c).

QUESTION 4:

A simple packet analyzer tool such as Wireshark can capture login credential of a user if the login page is using the following Protocol:

a. HTTP
b. SSH
c. HTTPS
d. SSL
e. None of these.

Correct Answer: a

Detail Solution: Wireshark can capture credentials of webpages which uses unsecure protocols such as HTTP, FTP.

The correct option is (a).

QUESTION 5:

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

a. By checking the ARP entry.
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: a, c

Detail Solution: By manually checking the ARP entry we can identify if any system is using same MAC address as the MAC of default gateway, which basically indicates that that particular system is configured in the promiscuous mode.

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 options are (a) and (c).

QUESTION 6:

What is the purpose of scanner module available in burp suite?

a. It is used to mount password attack.
b. It is used for manipulating and reissuing packets and to analyze their response.
c. It is used for creating dictionary.
d. It is used for automotive crawling web applications.
e. None of these.

Correct Answer: e

Detail Solution: Scanner module is used for finding vulnerabilities in web applications.

The correct option is (e).

QUESTION 7:

In Burp suite which of the following module is used to intercept, inspect and modify raw traffic?

a. Spider
b. Scanner
c. Intruder
d. Proxy
e. None of these.

Correct Answer: d

Detail Solution: Spider module is used for automotive crawling, scanner is used for vulnerability scanning, intruder is used for automatic customized attack against web application, proxy module gives a direct view of how target application works by working as proxy server. It gives facility to intercept, inspect and modify raw traffic of the application.

The correct option is (d).

QUESTION 8:

Which of the following is/are example(s) of computer-based social engineering attack?

a. Impersonation
b. Tailgating
c. Shoulder surfing
d. Chain letters
e. phishing

Correct Answer: d, e

Detail Solution: The options (a), (b) and (c) are example of human-based social engineering attacks, while d and e are examples of computer-based social engineering attack.

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

QUESTION 9:

How does Slowloris attack work?

a. It sends a single large ping packet to victim system.
b. It sends multiple HTTP requests to the victim system but never completes the request.
c. It sends large number ARP packet to the victim system.
d. None of these.

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 10:

Which of the following tools can be used to mount DoS attack?

a. LOIC tool.
b. Hping3.
c. Hydra.
d. Crunch.
e. None of these.

Correct Answer: a, b,

Detail Solution: LOIC and Hping3 tools can be used for DoS attack, Hydra and Crunch are used for password attack.

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

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