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:

What is the main objective of ethical hacking?

a. Deletes files from a system.
b. Inserts malwares in a system.
c. Legally Identify system vulnerabilities.
d. Steal sensitive information.

Correct Answer: c

Detail Solution: Ethical hacking involves simulating the actions of a malicious hacker to identify security vulnerabilities, but legally and with permission. This helps organizations strengthen their defenses.

Thus the correct option is (c).

QUESTION 2:

Which of the following are types of penetration testing methodologies?

a. White Box
b. Black Box
c. Red Box
d. Trojan Horse

Correct Answer: a, b

Detail Solution: There are mainly 3 methodologies are used for penetration testing; (a) white box model: in which the tester has complete information about the network, (b) black box model in which tester does not have any information about the network, (c) gray box model in

which partial information about the network is provide to tester. There is nothing called red box model. Trojan Horse is a malware technique.

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

QUESTION 3:

Which of the following switching techniques is more efficient for bursty data traffic?

a. Circuit Switching
b. Message Switching
c. Packet Switching
d. None of these

Correct Answer: c

Detail Solution: Packet switching allows multiple communications over shared links (dynamic bandwidth), making it suitable for bursty data. Circuit switched network is acceptable for voice communication but is very inefficient for high traffic like data streaming. In Message switching store-and-forward approach is used which incurs higher delay.

Thus, option (c) is true.

QUESTION 4:

Which protocol in TCP/IP is connectionless and does not provide reliability?

a. TCP
b. UDP
c. FTP
d. TELNET

Correct Answer: b

Detail Solution: UDP sends datagrams without establishing a connection and thus it is fast but unreliable. TCP, FTP and TELNET are connection oriented in which connection is established prior otodata transfer.

Thus, the correct option is (b).

QUESTION 5:

Which IP header field prevents infinite looping of packets?

a. Header Checksum
b. Time to Live
c. Fragment offset
d. HLEN

Correct Answer: b

Detail Solution: Time to Live **(**TTL) value is decremented at each router hop, and when it reaches 0, the packet is discarded. HLEN defines the header length, header checksum is used for header integrity, fragment offset is used for reassembling of packets.

Thus, the correct option is (b).

QUESTION 6:

What are the responsibilities of the IP layer?

a. Framing
b. Route packets
c. Provide reliable transmission
d. None of these

Correct Answer: b

Detail Solution: The transport layer provides reliability in transmission. The IP layer handles routing and addressing, framing and error-detection is handled by data-link layer.

Thus the correct option is (b).

QUESTION 7:

Which of the following is/are not a valid field of IP header?

a. TTL
b. Port Number
c. Protocols
d. MAC address

Correct Answer: b, d

Detail Solution: TTL prevents looping, whereas Protocols defines the protocols used in upper layer. Port number is a field of transport layer. MAC address is added in data-link layer.

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

QUESTION 8:

Which of the following statements is/are ***true*** about datagram packet switching?

a. Requires prior route establishment.
b. Faster for fewer packet.
c. Uses dynamic routing.
d. All packets follow the same path.

Correct Answer: b, c

Detail Solution: Datagram packets are independent, routed dynamically and can follow different paths. It does not require prior route establishment. As it does not require route establishment and termination, it is considered faster to transmit fewer packets.

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

QUESTION 9:

The max value (in decimal) for HLEN field (header length) is _____.

Correct Answer: 15

Detail Solution: for HLEN 4-bits are used; thus the max value which can be assigned is 1111 = 15.

QUESTION 10:

The header checksum field in the IP header is _____ bits wide.

Correct Answer: 16

Detail Solution: The header checksum which is used for header integrity is 16-bit wide.

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

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 do we need fragmentation?

a. To increase transmission speed.
b. Due to varying MTU across networks.
c. To improve encryption.
d. To compress packet.

Correct Answer: b

Detail Solution: If MTU is small and the packet is large then it cannot be transmitted through that network, and thus we need to divide the packet into smaller fragments. Thus we can say that fragmentation is required because MTU across network varies.

Thus the correct option is (b).

QUESTION 2:

IP fragmentation is typically done by:

a. Source Host
b. Destination Host
c. Intermediate Routers
d. Hubs

Correct Answer: c

Detail Solution: Fragmentation is performed by intermediate routers, while the reassembly of packets is done by the final destination host.

Thus the correct option is (c).

QUESTION 3:

For reassembling the fragmented packets at the final destination, which of the following header field(s) is(are) used?

a. Fragment offset
b. Flags
c. Port number
d. Checksum
e. Identification

Correct Answer: a, b, e

Detail Solution: For fragment assembly, identification (ID), fragment offset and flag fields are used.

Thus true options are (a), (b) and (e).

QUESTION 4:

An IP packet arrives at the final destination with the D flag set as 0, M flag set as 1 and offset is set to 0. Which of the following statements is **true** about the packet?

a. The packet has not been fragmented.
b. The packet has been fragmented and it is the first fragment.
c. The packet has been fragmented and it is the last fragment.
d. None of these.

Correct Answer: b

Detail Solution: D = 0 means fragmentation is allowed. 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, M=0 indicates the last fragmented packet. Offset = 0 indicates that it is the first fragmented packet.

Thus the true option is (b).

QUESTION 5:

In an IP packet, the value of HLEN is 15, and the total size of IP packet is 2000 bytes. The number of data bytes in the packet will be _____.

Correct Answer: 1930 to 1950

Detail Solution: Since HLEN = 15, the size of the IP header will be 15 x 4 = 60 bytes. The total size of the IP packet is given as 2000 bytes. Hence, the number of data bytes = 2000 – 60 = 1940 bytes.

QUESTION 6:

Which address classes do the IP addresses 128.0.1.3 and 193.11.23.10 belong to?

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

Correct Answer: b

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 128.0.1.3, the first byte 128 = **10**000000 in binary; for the IP address 193.11.23.10, the first byte 193 = **110**00001 in binary. Clearly, the first one is Class B, and the second one is Class C address.

Hence, the correct option is (b).

QUESTION 7:

Which IP addresses are reserved for private use?

a. 10.x.x.x
b. 172.32.x.x
c. 192.168.x.x
d. 128.x.x.x

Correct Answer: a, c

Detail Solution: 10.x.x.x, 172.16.x.x and 192.168.x.x are reserved for private use.

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

QUESTION 8:

What does a TCP segment with SYN =1 and ACK = 0 indicate?

a. Connection termination
b. Connection reset
c. Keep-alive signal
d. Initial connection request
e. Connection acknowledgement

Correct Answer: d

Detail Solution: In the TCP header, SYN=1 and ACK=0 represents connection request (first step of TCP 3-way handshake), whereas SYN=1 and ACK=1 represents connection confirmation. RST is used to reset/reject connection.

Thus correct option is (d).

QUESTION 9:

What is the size of UDP header?

a. 16 bits
b. 16 bytes
c. 8 bits
d. 8 bytes

Correct Answer: d

Detail Solution: UDP header size is 8 bytes (4 fields each of 16 bits).

Thus correct option is (d).

QUESTION 10:

What is the subnet address if the destination IP address is 192.168.77.213 and the subnet mask is 255.255.252.0?

a. 192.168.76.0
b. 192.168.76.213
c. 192.168.77.0
d. 192.168.0.0

Correct Answer: a

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

```
192.168.77.213 = 11000000 10101000 01001101 11010101
255.255.252.0  = 11111111 11111111 11111100 00000000
```

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

```
11000000 10101000 01001100 00000000 = 192.168.76.0
```

Thus the correct option is (a).

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

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 statement(s) is/are **false**? **[MSQ]**

a. IP protocol uses connection-oriented routing.
b. IP protocol uses connection-less routing.
c. In connection-less routing, each packet is treated as an independent packet.
d. None of these.

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:

A routing table entry that is manually configured remains unchanged unless manually modified is called a _____ routing table entry. **[MCQ]**

a. Automatic
b. Static
c. Dynamic
d. None of these

Correct Answer: b

Detail Solution: Static routing table entries are configured manually and does not change with time.

Thus the correct option is (b)

QUESTION 3:

Which of the following statements is/are **false** about *direct and indirect packet delivery*? **[MSQ]**

a. Direct delivery happens within the same network.
b. Indirect delivery is used for different networks.
c. In indirect delivery packet travel through multiple routers.
d. None of these.

Correct Answer: d

Detail Solution: Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host. If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.

Thus the correct options is (d).

QUESTION 4:

Which of the following statements correctly describe features of dynamic routing? **[MSQ]**

a. All routers are manually configured by the network administrator.
b. Routing table updates periodically depending on the network condition.
c. Routers exchange control information, which consumes network resources.
d. It can automatically find alternate paths during link failures.
e. It never changes the routing table once initialized.

Correct Answer: b, c, d

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. In dynamic routing routes are updated automatically based on the network condition. In dynamic routing some bandwidth are consumed for communication. In case of link failure; in static routing the administrator needs to update the routing table, whereas in dynamic routing the tables can be updated automatically, thus re-routing is easy.

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

QUESTION 5:

In the routing table, which of the following flags indicates that the route uses a gateway to reach the destination? **[MCQ]**

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

Correct Answer: b

Detail Solution: The G flag in a routing table stands for Gateway. It indicates that the route uses an intermediate gateway (router) instead of being directly connected. U means the route is up. H specifies a host-specific route. D and M indicates the route was dynamically created (modified) routing.

Hence, the correct option is (b).

QUESTION 6:

Which of the following statement about the default route is **incorrect**? **[MCQ]**

a. It is specified by an address 0.0.0.0.
b. It is specified by an address 127.0.0.1.
c. It is used for forwarding packets to unknown destinations.
d. None of these.

Correct Answer: 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 entry in the routing table. In IPv4 the CIDR notation for a default route is 0.0.0.0/0.

The incorrect option is (b).

QUESTION 7:

Which of the following routing protocols suffers from the count-to-infinity problem? **[MCQ]**

a. OSFP
b. BGP
c. RIP
d. None of these.

Correct Answer: c

Detail Solution: RIP uses distance vector routing which is prone to routing loops and can cause count-to-infinity problem.

The correct option is (c).

QUESTION 8:

Which of the following routing protocols is used for routing between different autonomous systems? **[MCQ]**

a. RIP
b. OSFP
c. BGP
d. ICMP

Correct Answer: c

Detail Solution: BGP is used for routing between different autonomous systems. RIP and OSFP are interior protocols, ICMP is not a routing protocol.

The correct option is (c).

QUESTION 9:

In Open Shortest Path First (OSPF) routing protocol, which of the following packets is used to check if the neighbor router is up(active)? **[MCQ]**

a. Link State Request
b. Hello Packet
c. Link State Acknowledgement

d. TCP 3-way handshake
e. None of these

Correct Answer: b

Detail Solution: In Open Shortest Path First (OSPF) routing approach, the "Hello" packet is used to check if a neighbor is up or not.

Thus, the correct option is (b).

QUESTION 10:

Which of the following statement(s) is/are **false** for IPv6? **[MSQ]**

a. IPv6 supports address class like A, B, and C.
b. IPv6 address are 128-bit long.
c. The base header size in IPv6 is 40 byte.
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. Base header size of IPv6 is 40 bytes it is represented by hexadecimal numbers separated by (:).

Thus the false statement is option (a).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Ethical Hacking

Assignment- Week 4

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1:

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

a. A hypervisor allows one host to run multiple virtual machines by sharing resources.
b. A hypervisor requires one physical machine per virtual machine.
c. A hypervisor can only run one virtual machine at a time.
d. Kali-linux is hack proof hypervisor.
e. None of these.

Correct Answer: a

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; each system can use the resources of main system (host system) such as memory, network interface, storage etc. This is very essential for security practice. 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 (a).

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 the information is collected indirectly, i.e. web browsing. The attacker and victim do not communicate directly, and thus there is no chance of detection. In active reconnaissance, we collect information about a target directly, e.g., nmap scan. As the attacker and victim communicate directly, there is a chance of detection.

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

QUESTION 3:

Which operator is used in Google to search for an exact phrase?

a. AND
b. " " (double quotes)
c. +
d. ()

Correct Answer: b

Detailed Solution: Putting a phrase inside double quotes tells Google to search for that exact sequence of words in that order.

The correct option is (b).

QUESTION 4:

What does a WHOIS lookup provides?

a. Website loading speed.
b. Source code of webpage
c. Historical screenshot of website
d. Ownership and registration details of a domain.

Correct Answer: d

Detailed Solution: WHOIS is a tool used to find details like domain owner name, registrar, registration date, and expiration date.

The correct option is (d).

QUESTION 5:

Which search will show results from only the website swayam.gov.in?

a. swayam.gov.in
b. filetype:swayam.gov.in
c. site:swayam.gov.in
d. None of these

Correct Answer: c

Detailed Solution: just writing the website may show result from other websites as well, site operator limits the search to a specific website or domain, filetype operator filters by file type and not domain.

The correct option is (c).

QUESTION 6:

What is the main function of Archive.org's Wayback Machine?

a. To view historical version of the website
b. To scan website for malware
c. To test internet speed.
d. To monitor websites uptime

Correct Answer: a

Detailed Solution: The Wayback Machine allows users to see snapshots of websites from the past, useful for research, legal reference, or digital preservation.

The correct option is (a).

QUESTION 7:

An ICMP sweep scan is used to:

a. Block TCP connection
b. Scan for DNS servers
c. Detect live hosts
d. Detect phishing emails.

Correct Answer: c

Detailed Solution: ICMP sweep scan is used to detect live hosts in a network. 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 (c).

QUESTION 8:

Which of the following tools is primarily used for network scanning, including host discovery and port scanning?

a. Wireshark
b. DNSEnum
c. Notepad++
d. None of these

Correct Answer: d

Detailed Solution: Wireshark is a packet capturing and analysis tool — it does not perform scanning (like discovering hosts or ports). DNSEnum is used for DNS enumeration, not general port or host scanning. Notepad++ is simply a text/code editor. Tools like Nmap and Nessus are specifically used for network scanning, including host discovery and port scans.

The correct option is (d).

QUESTION 9:

Which of the following option tells NMAP to skip port scanning and perform only host discovery?

a. –sS
b. –O
c. -sn
d. -p

Correct Answer: c

Detailed Solution: -sn tells Nmap to skip port scanning and perform only host discovery (also known as ping scan). -sS → SYN scan (port scan); -O → OS detection; -p → specifies ports to scan.

The correct option is (c).

QUESTION 10:

How many ports does NMAP scan by default when no specific port option is provided_____?

Correct Answer: 1000

Detailed Solution: Nmap scans the 1,000 most commonly used ports by default for TCP and UDP.

********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: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Where are the default NMAP scripts stored in a typical Linux system?

a. /usr/bin/nmap/scripts
b. /usr/share/nmap/scripts
c. /opt/nmap/ scripts
d. /etc/ nmap/scripts

Correct Answer: b

Detail Solution: On Linux, the default NSE script directory is: /usr/share/nmap/scripts

The correct option is (b).

QUESTION 2:

Which of the following NMAP options runs the default set of NSE scripts?

a. --nse
b. --script=all
c. --script=default
d. --run-default

Correct Answer: c

Detail Solution: --script=default runs the standard/default set of scripts designed for version detection, service discovery, basic vulnerabilities, and more. --script=all runs all available scripts (not recommended unless needed).--nse and --run-default are invalid or non-existent options.

The correct option is (c).

QUESTION 3:

Which of the following NMAP scripts checks for vulnerabilities to a Slowloris DoS attack?

a. http-slowloris-test
b. http-slowloris-discovery
c. http-slowloris-check
d. http-slowloris-flood
e. None of these

Correct Answer: c

Detail Solution: http-slowloris-check script is used to check if the webserver is vulnerable to DoS attack without actually launching a DoS attack, http-Slowloris script is used to launch Slowloris attack. There is no script with name http-slowloris-test or flood.

The correct option is (c).

QUESTION 4:

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

a. http-os-brute
b. smb-os-brute
c. smb-brute
d. smb-os-attack
e. None of these

Correct Answer: e

Detail Solution: Nmap does not have a script named http-os-brute, smb-os-brute, smb-brute, or smb-os-attack. The correct script for OS identification via SMB is smb-os-discovery, which is not listed.

The correct option is (e).

QUESTION 5:

Which of the following best describes the function of the crunch tool in hacking?

a. It scans open ports and running services on a target system.
b. It generates custom wordlist for password attacks.
c. It hashes passwords using various algorithms.
d. It decrypts SSL/TLS encrypted traffic.
e. None of these.

Correct Answer: b

Detail Solution: Crunch is used to create custom password dictionaries based on rules like length, character set, prefixes/suffixes, etc.

Thus the correct option is (b).

QUESTION 6:

What is the primary function of the hydra tool in penetration testing?

a. Generating custom wordlist for password attacks.
b. Performing OS fingerprinting
c. Performs ARP spoofing attacks
d. Brute-force login attempts on network services

Correct Answer: d

Detail Solution: Hydra is a fast and flexible login cracker that supports many protocols: SSH, FTP, HTTP, SMB, MySQL, Telnet, etc.

Thus the correct option is (d).

QUESTION 7:

Which tool is most appropriate for performing a brute-force attack against remote login services such as Telnet, FTP, or SSH?

a. DNSEnum
b. Crunch
c. Hydra
d. Wireshark

Correct Answer: c

Detail Solution: Hydra is a popular login brute-forcer that supports multiple services like Telnet, FTP, SSH, HTTP, SMB, etc. Crunch generates wordlists but does not perform attacks. Wireshark captures network traffic. DNSEnum is used for user enumeration.

Thus the correct option is (c).

QUESTION 8:

What is user enumeration?

a. Creating multiple user accounts on a system.
b. Deleting inactive user accounts
c. Identifying valid usernames on a target system or services
d. None of these.

Correct Answer: c

Detail Solution: User enumeration is the process of determining valid usernames on a system, often by analyzing different responses from login attempts or error messages.

The correct option is (c).

QUESTION 9:

Which malware records the keystrokes that are typed on the keyboard?

a. Keylogger
b. Virus
c. Adware
d. None of these.

Correct Answer: a

Detail Solution: A Keylogger monitors and records every keystroke made on a keyboard. It is often used by attackers to steal passwords, credit card numbers, and other sensitive information.

The correct option is (a).

QUESTION 10:

Which of the following best describes the function of the ARP (Address Resolution Protocol)?

a. It maps IP addresses to MAC addresses in a local network.
b. It encrypts data at the transport layer.
c. It maps domain names to IP addresses.
d. It establishes secure tunnels between routers.

Correct Answer: a

Detail Solution: ARP is used to find the MAC address corresponding to an IP address within a local subnet. It works at the Network Layer (Layer 3) interacting with the Data Link Layer (Layer 2).

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:

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 2:

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

a. In symmetric key cryptography, separate keys are used by sender and receiver.
b. In symmetric key cryptography, a single key is used by sender and receiver.
c. In asymmetric key cryptography, separate keys are used by sender and receiver.
d. In asymmetric key cryptography, a single key is used by sender and receiver.

Correct Answer: a, d

Detail Solution: Encryption is the most important concept for network security, and typically two types of encryptions are used. Private key (symmetric): where the sender and receiver uses same key for encryption/decryption of the message. Public key (asymmetric): where separate keys are used for encryption and decryption of the message.

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

QUESTION 3:

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.

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 4:

100 parties want to exchange messages securely using public-key cryptography (like RSA). The number of distinct key values required will be _____.

Correct Answer: 200

Detail Solution: In asymmetric encryption, every party have two keys (private and public) For N parties, the number of keys will be 2N = 2 x 100 = 200.

QUESTION 5:

20 parties want to exchange messages securely using symmetric key cryptography. The number of distinct key values required will be _____.

Correct Answer: 190

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 = 20, ${}^{20}C_2 = 20 \times 19 / 2 = 190$.

QUESTION 6:

We want to encrypt the plain text "CRYPTOGRAPHY" using a substitution cipher, where each letter is replaced by the k-th next letter, with the following assumptions:

(i) The alphabets are wrapped around, i.e. Z is followed by A.

(ii) Each alphabet (A to Z) is assigned a number (1 to 26).

(iii) The value of secret key k is 4.

What will be the cipher text?

a. GWCUXSKWETMC
b. GVCTXSKVETLC
c. HTDZAXLYIXPG
d. KZRVUOCPJQNA
e. None of these.

Correct Answer: b

Detail Solution: k=4 indicates that for encryption, each letter is replaced by its 4th following letter (C → G, R → V, Y → C, P → T, T → X, O → S, G → K, R → V, A → E, P → T, H → L, Y → C.) If we encrypt the message we will get the cipher text as GVCTXSKVETLC.

Thus the correct option is (b).

QUESTION 7:

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

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

What will be the encrypted form of the message "SWAYAM" ?

a. GCAYAM
b. SWAYAM
c. WCAYAM
d. None of these.

Correct Answer: a

Detail Solution: According to the specified mapping the encrypted message will be GCAYAM.

Hence, the correct option is (a).

QUESTION 8:

If a receiver A wants to carry out decryption on a message received from B using public-key cryptography, which of the following key will be used for decryption by A?

a. A's public key
b. A's private key
c. B's public key
d. B's private key

Correct Answer: b

Detail Solution: If a receiver A wants to carry out decryption on a message received from B, using public-key cryptography, that means B must have encrypted the message using A's public key which can be decrypted using A's private key.

Thus the correct option is (b).

QUESTION 9:

AES uses an effective key length of _____ bits?

a. 64 bit
b. 128 bit
c. 192 bit
d. 256 bit
e. 513 bit.

Correct Answer: b, c, d

Detail Solution: In AES the block length is limited to 128-bit; however, the key length can be 128, 192 or 256 bits.

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

QUESTION 10:

Which cryptographic algorithms uses the same key for encryption and decryption?

a. RSA
b. Diffie-Hellman
c. DES
d. AES

Correct Answer: c, d

Detail Solution: both DES and AES are symmetric key algorithms which uses same key for encryption and decryption.

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

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

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 type of mapping is implemented by cryptographic hash function?

a. One-to-One

b. Many-to-One

c. One-to-Many

d. Many-to-Many

Correct Answer: b

Detail Solution: A hash function takes a message of arbitrary length and generates a fixed length Hash. That means the input set is very large and output set is finite which makes it many to one mapper.
The correct option is (b).

QUESTION 2:

Two messages M_1 and M_2 are fed to a hash function HASH to generate the hash value:

H_1 = HASH (M_1)

H_2 = HASH (M_2)

Which of the following options can **never be true**?

a. $H_1 = H_2$ and $M_1 != M_2$

b. $H_1 != H_2$ and $M_1 = M_2$

c. $H_1 != H_2$ and $M_1 != M_2$

d. $H_1 = H_2$ and $M_1 = M_2$

Correct Answer: b

Detail Solution: A hash function is deterministic (same input always gives same output) Thus if $M_1 = M_2$; H_1 must be equal to H_2. Two different messages M1 and M2 can, however, generate the same hash value, which is called collision.

The correct option is (b).

QUESTION 3:

Which of the following is true for hash function?

a. Hashing can be reversed.
b. Hash function generates a variable length output.
c. It is computationally easy to find collisions
d. None of these.

Correct Answer: d

Detail Solution: A hash function has the following properties: one way → non-reversible, fixed-length output, and collision resistance (computationally hard to detect collision).

The correct option is (d).

QUESTION 4:

Which of the following is provided by Unkeyed hash function (Modification Detection Code)?

a. Integrity
b. Authenticity
c. Confidentiality
d. Availability

Correct Answer: a

Detail Solution: Unkeyed hash function takes an input of variable length and converts it to a fixed-length output. It is designed to detect if the message has been altered during transmission or not. Any change in message will cause change in hash thus it ensures integrity. Since no key is used it does not provide authenticity. As the message is not encrypted it does not provide confidentiality. Availability is not related with hashing.

Thus the correct option is (a).

QUESTION 5:

Which of the following are UNKEYED hash functions?

a. MD5
b. HMAC
c. SHA-256
d. CMAC

Correct Answer: a, c

Detail Solution: MD5 and SHA-256 are examples of Unkeyed hash function, while HMAC and CMAC are example of keyed hash function.

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

QUESTION 6:

SHA-512 processes the message in _____ bits blocks.

Correct Answer: 1024

Detail Solution: SHA-512 process the message in a block of 1024 bits.

QUESTION 7:

Which type of digital signature generates the same signature every time for a given message?

a. Deterministic Signature
b. Probabilistic Signature
c. Blind Signature
d. Undeniable Signature

Correct Answer: a

Detail Solution:

Deterministic signatures → for a given message, the signing algorithm always produces the same signature.
Probabilistic signatures → use randomization, so even for the same message, different runs of the algorithm generate different signatures.
Blind signatures → signer does not see the content of the message being signed.
Undeniable signatures → require the active participation of the signer during verification.

The correct option is (a).

QUESTION 8:

Which property of digital signature ensures that a signer cannot deny a valid signature created by them?

a. Confidentiality
b. Integrity
c. Non-repudiation
d. Availability

Correct Answer: c

Detail Solution: Digital signatures provide three key security services:
Integrity: Ensures the message has not been altered.
Authentication: Confirms the sender's identity.
Non-repudiation: Prevents the sender from denying that they signed the message.

Non-repudiation specifically means → Once a signer digitally signs a message with their private key, they cannot later claim they did not sign it. The signature can be verified by anyone using the signer's public key, proving it was generated by the signer.

The correct option is (c).

QUESTION 9:

Which of the following is not an objective of SSL?

a. Authentication
b. Data Integrity
c. Data Privacy
d. Faster Transmission

Correct Answer: d

Detail Solution: Main objectives of SSL are:
Authentication → the client and server authenticate each other using certificates/keys.
Data Integrity → ensures data is not altered during transmission.
Data Privacy (Confidentiality) → Protects data using encryption so that only intended parties can read it.
Faster transmission is not an objective of SSL.
The correct option is (d).

QUESTION 10:

In IPSec, which mode encapsulates only the transport layer information with protection?

a. Tunnel Mode
b. Transport Mode
c. Replay Mode
d. Confidential Mode

Correct Answer: b

Detail Solution: IPSec provides two modes of protection:
Tunnel Mode → Encapsulates the entire IP packet (header + payload).
Transport Mode → Encapsulates only the transport layer information (payload), while leaving the original IP header intact.
Replay and Confidential are not a mode in IPSec's standard terminology.

The correct answer is (b)

**********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 one of the following best describes steganography?

a. Use encrypting/decryption technique so that data can be read only by intended recipient.
b. Hiding the existence of a message by embedding it inside another medium (audio/video/image).
c. Digitally sign a message to provide authenticity.
d. Compress data to reduce transmission size.

Correct Answer: b

Detail Solution: Steganography is the art of hiding the existence of a message by embedding it within another medium (image, audio, video, executable, etc.).

Thus the correct option is (b).

QUESTION 2:

Which of the following is/are true about LSB steganography in images?

a. It is simple to implement.
b. It is robust against lossy compression like JPEG.
c. It works well with 24-bit images.
d. It is vulnerable to image manipulation and filtering.

Correct Answer: a, c, d

Detail Solution: LSB steganography is straightforward and easy to implement. In JPEG compression the LSB bits are easily lost during compression, so it is not robust against it. More

bits per pixel → higher hiding capacity. Format conversion or filtering may also destroy the LSB, i.e. the hidden message.

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

QUESTION 3:

Consider a RGB image of size 200 x 150, where each pixel is stored in 24-bits (3-color channels, 8-bits each). The number of ***bytes*** of information that can be hidden in the image using LSB steganography (replacing 1 LSB-bit in each channel of every pixel) is _____.

Correct Answer: 11250

Detail Solution: Each pixel consists 3 channels, and hence 3 bits of information can be stored in each pixel. The number of bytes of hidden information that can be stored in the whole image can be calculated as follows.

Total number of pixels = 200 x 150 = 30,000

Total number of bytes that can be hidden = 30000 x 3 / 8 = 11250 bytes

---

QUESTION 4:

Which of the following does not correspond to physiological biometrics?

a. Fingerprint
b. Iris
c. Retina
d. Signature

Correct Answer: d

Detail Solution: Physiological biometrics are physical body features (fingerprint, iris, retina, etc.). Signature dynamics, keystroke patterns and gait are behavioral biometrics.

The correct option is (d).

QUESTION 5:

Which biometric gives the highest uniqueness for identification but is often invasive?

a. Face
b. Voice
c. Signature
d. Iris/Retina

Correct Answer: d

Detail Solution: Iris and retina patterns are highly unique per individual and between eyes; retina recognition is particularly strong though it can be intrusive and stressful to subject. Face, voice and signature are less unique and more environment-dependent.

The correct option is (d)

QUESTION 6:

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 modifies the stored password information in a system.
d. None of these.

Correct Answer: b

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

QUESTION 7:

A Smurf DoS attack works by:

a. Sending oversized IP packets to crash a host.
b. Sending forged ICMP echo requests to a broadcast address so that many hosts reply to the spoofed victim IP.
c. Exploiting a buffer overflow in web servers.
d. Using SQL injection to compromise database.

Correct Answer: b

Detail Solution: Smurf sends ICMP Echo requests to a network broadcast address, with the source address spoofed to the victim; many hosts reply to the victim and flood it. Oversized packets describe Ping-of-Death.

The correct option is (b).

QUESTION 8:

Which of the following is an example of denial-of-service attack?

a. Ping-of-death
b. SQL injection
c. Phishing
d. Smurf attack

Correct Answer: a, d

Detail Solution: (a) and (d) are examples of denial-of-service attack.

QUESTION 9:

What is the main purpose of Domain Name System (DNS)?

a. To provide end-to-end encryption for emails.
b. To map human-readable domain names to IP addresses.
c. To compress and segment long messages.
d. To hide secret data inside images.

Correct Answer: b

Detail Solution: DNS translates human-readable names (like www.google.com) into machine-usable IP addresses. This enables users to access websites using domain names instead of remembering numeric IPs.

The correct option is (b).

QUESTION 10:

A Distributed Denial-of-Service (DDoS) attack differs from DoS primarily because:

a. DDoS targets multiple victim servers at once.
b. DDoS uses multiple compromised machines (botnet) to attack a single target, increasing scale and obfuscation.
c. DDoS only uses UDP while DoS uses TCP.
d. There is no difference between DDoS and DoS.

Correct Answer: b

Detail Solution: DDoS involves many coordinated attackers (botnet) making tracing and mitigation harder; it is about multiple sources attacking one target. It is not limited to a specific protocol.

The correct option is (b).

**********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:

Which mode allows a network interface card (NIC) to capture all traffic on the network segment regardless of the destination?

a. Monitor mode
b. Transparent mode
c. Promiscuous mode
d. Hypervisor mode

Correct Answer: c

Detail Solution: When using sniffing tools like Wireshark, the NIC is set to promiscuous mode, allowing it to capture all packets on the segment, not just those destined for the host.

The correct option is (c).

QUESTION 2:

Which of the following is/are not a feature of Wireshark?

a. Captures and analyzes packets
b. Generates statistical reports
c. Manipulates live network traffic
d. Carries out SQL injection attack

Correct Answer: c, d

Detail Solution: Wireshark can capture, analyze, and display packets with GUI support, and also generate statistical reports. But it cannot manipulate live traffic — tools like Ettercap or BurpSuite are used for that, SQL injection is not a feature of Wireshark.

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

QUESTION 3:

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 exchange data in plain text (unsecured form), and thus they are vulnerable to sniffing attack.

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

QUESTION 4:

Which of the following countermeasures is effective against sniffing attacks?

a. Use switch instead of hub
b. Use Telnet instead of SSH
c. Disable HTTPS
d. Allow ARP broadcasts

Correct Answer: a

Detail Solution: A switch forwards packets only to intended recipients, limiting the scope for sniffing. Using telnet and disabling HTTPS can increase the risk of sniffing.

The correct option is (a).

QUESTION 5:

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

Correct Answer: a, b, c

Detail Solution: The Ettercap tool can carry out IP-based filtering, MAC-based filtering, and 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 6:

Which of the following is an example of reverse social engineering?

a. Attacker pretends to be IT support so victim voluntarily provides information
b. Attacker steals password by shoulder surfing
c. Attacker sends phishing mail
d. Attacker sneaks in through tailgating

Correct Answer: a

Detail Solution: In reverse social engineering, the attacker acts as an authority, and the victim approaches the attacker for help, revealing sensitive info.

The correct option is (a).

QUESTION 7:

Which of the following is NOT a human-based social engineering attack?

a. Impersonation
b. Shoulder surfing
c. Piggybacking
d. Phishing

Correct Answer: d

Detail Solution: Phishing is a computer-based social engineering attack. The others are example of direct human-based attacks.

The correct option is (d).

QUESTION 8:

A DoS attack that exploits the TCP three-way handshake is called:

a. SYN Flooding
b. ICMP Flood
c. Ping of Death
d. UDP Flood

Correct Answer: a

Detail Solution: SYN Flooding sends repeated SYN requests without completing handshakes, exhausting server listen queues.

The correct option is (a).

QUESTION 9:

Which tool performs a DoS attack by sending partial HTTP requests and never completing them?

a. Hydra
b. Wireshark
c. Slowloris
d. Crunch

Correct Answer: c

Detail Solution: Slowloris opens many connections with partial requests, keeping them alive and exhausting server resources.

The correct option is (c).

QUESTION 10:

Which of the following best defines a Botnet?

a. A network of legitimate IoT devices
b. A protocol for DoS mitigation
c. A security feature in switches
d. A group of compromised systems remotely controlled by an attacker

Correct Answer: d

Detail Solution: A botnet is a large network of compromised machines under attacker control, often used to launch DDoS attacks.

The correct option is (d).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 10

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which of the following is/are not an example of hardware-based attack?

a. Side-channel attack
b. Physical probing
c. Denial of service
d. SQL injection

Correct Answer: c, d

Detail Solution: In side-channel attack, some side channels (like delay, power, etc.) are monitored during some computation using some sophisticated measuring instruments, and as such requires access to the hardware that runs the computation. In comparison, denial-of-service and SQL injection are essentially software-based attacks.

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

QUESTION 2:

Which of the following are typically exploited in side-channel attacks?

a. Time required to carry out operations
b. Electromagnetic emissions from the device
c. Space complexity of the algorithm
d. Plaintext and Ciphertext
e. Power consumed during computation

Correct Answer: a, b, e

Detail Solution: Timing analysis, power analysis, and EM emission analysis are very common in mounting side-channel attacks. It does not rely on the space complexity plaintext/ciphertext of the algorithm.

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

QUESTION 3:

Which of the following attacks on hardware are invasive in nature?

a. Black-box testing
b. Physical probing
c. Reverse engineering
d. Side-channel attack

Correct Answer: b, c

Detail Solution: Invasive attack → attack that needs direct physical access that alters or opens the chip/package.

Physical probing is invasive, it involves decapping the package or touching internal nodes with probes. Reverse engineering is invasive when it requires removing layers, imaging dies, or destructively extracting the netlist.

Black-box testing is non-invasive (tests only inputs/outputs). Side-channel analysis is typically non-invasive (measures power/timing/EM externally).

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

QUESTION 4:

Which of the following can be used as countermeasures to prevent hardware-based attacks?

a. Obfuscate data in register and buses
b. Add dummy circuit to generate random noise
c. Increase CPU clock frequency to make probing harder
d. Use secure cryptographic algorithm

Correct Answer: a, b

Detail Solution: Typical Countermeasures to Prevent Hardware Attacks are: Obfuscate data in registers, generate random noise generator to prevent side-channel attacks, add metal mesh on top of the circuit, secret hiding, PUF. Use of cryptographic algorithms is essential for data security but cannot mitigate hardware-based attacks. Increasing the CPU clock frequency cannot prevent attacks like side-channel attack, it may make it easy due to high electromagnetic emission

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

QUESTION 5:

What is hardware Trojan?

a. A virus that infects software
b. A malicious change inside a chip
c. A tool used for testing hardware
d. A feature to make hardware faster

Correct Answer: b

Detail Solution: A hardware Trojan is a hidden malicious modification in a chip that can cause it to leak data or misbehave.

The correct option is (b).

QUESTION 6:

Which of the following is/are true for differential power analysis?

a. It requires a single measurement
b. It requires multiple measurements
c. It is more effective than simple power analysis
d. It is less effective than simple power analysis

Correct Answer: b, c

Detail Solution: Differential power analysis is more sophisticated and effective as compared to simple power analysis. Differential power analysis requires multiple measurements.. The correct options are (b) and (c).

QUESTION 7:

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

a. Detection of hardware Trojans is relatively easy
b. No single method can detect all types of hardware Trojans
c. Hardware Trojan detection often involves high design, testing, or runtime overhead
d. Hardware Trojans are always inserted at the software level

Correct Answer: a, d

Detail Solution: Trojan detection is difficult; no single method can detect all types of Trojan; Trojan detection often adds significant overhead; Trojans are inserted at hardware level hardware.

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

QUESTION 8:

For modular exponentiation computation of x^{25}, how many squaring and multiplication operations would be required?

a. 3 and 2
b. 3 and 3
c. 3 and 4
d. 4 and 2

Correct Answer: d

Detail Solution: The binary representation of 25 is 11001.

Thus, $x^{25} = x^{16} * x^8 * x^1 = (((x^2 * x)^2)^2)^2 * x^1$

This computation requires 4 squaring and 2 multiplication operations.

Shortcut rule: Squaring → total bits – 1

: Multiplication → (#of 1's) - 1

The correct option is (d).

QUESTION 9:

What is the main purpose of Physical Unclonable Function (PUF) in hardware security?

a. To increase the clock speed of the processor
b. To provide device-unique authentication
c. To reduce the power consumption of chips
d. To improve signal transmission speed

Correct Answer: b

Detail Solution: PUFs exploit manufacturing variations to generate unique, unpredictable responses for each chip, making them useful for authentication and secure key generation.

The correct option is (b).

QUESTION 10:

Which of the following statements describe the evaluability property of PUF?

a. Given a PUF, it is hard to construct a procedure PUF', where PUF ≠ PUF', and PUF'(x) = PUF(x) for all x.
b. Given only y and corresponding PUF instance, it is hard to find x such that PUF(x) = y.
c. Given PUF and x, it should be easy to evaluate y = PUF(x).
d. None of these.

Correct Answer: c

Detail Solution: All the listed points are desirable properties of PUFs. Option (a) describes the unclonable property, option (b) describes the one-wayness property, while option (c) correctly describes the evaluability property.

The correct option is (c).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 11

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which of the following Metasploit modules is used to take advantage of a vulnerability on some target system?

a. Exploit
b. Payload
c. Auxiliary
d. Encoder
e. None of these

Correct Answer: a

Detail Solution: Encoder module is used to encode the payloads. Exploit module is used to take advantage of System/Application bugs (vulnerabilities). Payload module is used to establish communication channel between Metasploit framework and target system. Auxiliary module is used to perform brute force attack, DoS attack, host and port scanning, vulnerability scanning, etc.

The correct option is (a).

QUESTION 2:

Which of the following describes meterpreter accurately?

a. It is a static payload generator.
b. It is an interactive payload that allows remote commands and file operations.
c. It is a Metasploits web Graphical User Interface.
d. It is a network scanner bundled with Metasploit.
e. It is a database for storing exploits.

Correct Answer: b

Detail Solution: Meterpreter is a powerful payload that provides remote interactive access, file transfers, VNC, and privilege escalation support.

The correct option is (b)

QUESTION 3:

Which Metasploit option is used to set the remote target port?

a. Set LHOST
b. Set LPORT
c. Set RHOST
d. Set RPORT
e. None of these

Correct Answer: d

Detail Solution: LHOST = attacker machine IP, LPORT = local port, RHOST = target IP, RPORT = target port.

The correct option is (d).

QUESTION 4:

What is the purpose of the Metasploit Encoder module?

a. Scan for vulnerabilities
b. Escalate privileges on the target
c. Encode payloads to evade antivirus detection
d. None of these

Correct Answer: c

Detail Solution: Encoder encodes payloads to bypass Antivirus detection. It does not exploit or scan vulnerabilities.

The correct option is (c).

QUESTION 5:

Which SQLMAP option lists all database names on the target?

a. --dbs
b. --tables
c. --databases
d. --dump
e. --current-db

Correct Answer: a

Detail Solution: The option --dbs lists all available databases. --tables lists tables, --dump dumps entries, --current-db shows current DB.

The correct option is (a).

QUESTION 6:

Which of the following is **not** a type of SQL injection technique?

a. Error-based
b. Union query-based
c. Opcode injection
d. Boolean-based blind

Correct Answer: c

Detail Solution: Error-based, Boolean-based, time-based blind, and union query are SQL injection techniques. Opcode injection is unrelated to SQL.

The correct option is (c).

QUESTION 7:

Which of the following are valid Metasploit payload types?

a. Command shell
b. Meterpreter
c. Dynamic payloads
d. Static payloads
e. SQL payload

Correct Answer: a, b, c, d

Detail Solution: Metasploit includes command shell, Meterpreter, dynamic and static payloads. There is no "SQL payload."

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

QUESTION 8:

If any web page is vulnerable to blind SQL injection, then which of the following is true?

a. It will print error message for incorrect user input.
b. It will not print anything for incorrect user input.

Correct Answer: b

Detail Solution: If the webpage is vulnerable to error-based sql injection, then it will generate an error message for incorrect user input. If it is vulnerable to blind sql injection then it will not generate any output for incorrect user input.

The correct option is (b).

QUESTION 9:

Which of the following SQLMAP options can extract credential-related information?

a. - -users
b. - -passwords
c. - -current-user
d. - -hostname

Correct Answer: a, b, c

Detail Solution: SQLMAP can retrieve DB users, hashed passwords, privileges, and current-user. Hostname only returns DBMS host, not credentials.

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

QUESTION 10:

Which of the following are recognized types of XSS attacks?

a. Stored (persistent) XSS
b. Reflected (non-persistent) XSS
c. DOM-based XSS
d. SQL-based XSS
e. Cookie Injection XSS

Correct Answer: a, b, c

Detail Solution: Stored, reflected, and DOM are the three classical XSS forms. SQL-based XSS, and Cookie based XSS are invalid.

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

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 12

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which option is used for ICMP echo sweep in NMAP?

a. –PE
b. –PS
c. –PP
d. –PM

Correct Answer: a

Detail Solution: The -PE option is used for ICMP Echo requests (type 8). If replies are received, the host is alive.

The correct option is (a).

QUESTION 2:

In ICMP Sweep, receiving ICMP Type 0 reply indicates:

a. Target host is down
b. Target host is alive
c. Target host is filtered
d. None of these.

Correct Answer: b

Detail Solution: ICMP type 0 is Echo reply, if it is received that means the target is alive.

The correct option is (b).

QUESTION 3:

By default NMAP scans how many ports?

a. 10
b. 100
c. 1000
d. 65536

Correct Answer: c

Detail Solution: NMAP by default scans top 1000 ports.

The correct option is (c).

QUESTION 4:

Which option makes NMAP treat all host as online (skip host discovery)?

a. –SP
b. –PO
c. –Pn
d. –F

Correct Answer: c

Detail Solution: -Pn skips host discovery and treats all hosts as online.

The correct option is (c).

QUESTION 5:

Which scanning technique uses full 3-way handshake?

a. TCP SYN scan
b. TCP Connect scan
c. ICMP Sweep scan
d. FIN scan

Correct Answer: b

Detail Solution: TCP Connect scan (-sT) uses complete 3-way handshake. TCP SYN scan is half-open. FIN and ICMP are not related to TCP 3-way handshake.

The correct option is (b).

QUESTION 6:

Assume we are running Wireshark in a host, if the NIC of the host is set in promiscuous mode, what Wireshark will do:

a. It will capture packets only oriented to that host
b. It will capture all packets in the same network segment in which host is connected.
c. It will encrypt all captured packet.
d. It will block all malicious traffic.

Correct Answer: b

Detail Solution: Promiscuous mode allows NIC to capture all packets in the network segment, not just its own traffic.

The correct option is (b).

QUESTION 7:

Which of the following NMAP option is used for OS discovery?

a. –O
b. –TO
c. –SO
d. None of these

Correct Answer: a

Detail Solution: -O option enables OS detection in NMAP. There is no –TO, -SO option.

The correct option is (a).

QUESTION 8:

Which of the following can be detected using service/version detection (-sV)?

a. Application name
b. Application version
c. OS fingerprint
d. Vulnerability status

Correct Answer: a, b

Detail Solution: The -sV option probes open ports to detect the application name and version. OS fingerprinting is done with -O, and vulnerabilities require scripts.

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

QUESTION 9:

Which NMAP option allows scanning only the most common 10 ports?

a. – p 10
b. –r 10
c. – top-ports 10
d. –top 10

Correct Answer: c

Detail Solution: The --top-ports <N> option scans the most common N ports instead of the full range. –top is not a valid option, -r is for ordering/randomization, with –p only port 10 will be scanned.

The correct option is (c).

QUESTION 10:

In which default format does Wireshark save captured packets?

a. .txt
b. .csv
c. .xml
d. .pcapng/.pcap

Correct Answer: d

Detail Solution: Wireshark saves captured packets by default in .pcapng (Packet Capture Next Generation) format (.pcap in older version). It can also export to other formats (TXT, CSV, XML, JSON), but the default is .pcapng.

The correct option is (d).

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