Ethical Hacking

Assignment- Week 4

TYPE OF QUESTION: MCQ/MSQ

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

QUESTION 1:

What is the purpose of the Hypervisor software?

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

Correct Answer: c

Detailed Solution:

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

The correct option is (c).

QUESTION 2:

What are some of the features in Kali Linux?

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

Correct Answer: b

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

The correct option is (b).

QUESTION 3:

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

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

Correct Answer: a, c

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

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

QUESTION 4:

Which of the following can be used for passive reconnaissance?

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

Correct Answer: a, b, c, d

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

QUESTION 5:

How host discovery can be carried out using ICMP sweep?

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

Correct Answer: a

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

The correct option is (a).

QUESTION 6:

How does port scanning using TCP Connect works?

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

Correct Answer: b

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

The correct option is (b).

QUESTION 7:

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

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

Correct Answer: d

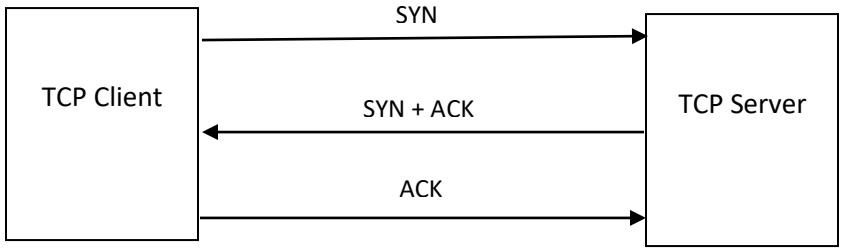
Detailed Solution: TCP connection establishment involves a 3-way handshake.

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

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

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

The correct option is (d).



QUESTION 8:

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

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

Correct Answer: b, d

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

QUESTION 9:

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

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

Correct Answer: b

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

The correct option is (b).

QUESTION 10:

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

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

Correct Answer: d

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

The correct option is (d).

QUESTION 11:

What is the purpose of the following NMAP command?

```
nmap –sn 192.55.70.110-120
```

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

Correct Answer: b

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

Thus, the correct option is (b).

QUESTION 12:

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

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

Correct Answer: a, b

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

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

QUESTION 13:

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

Correct Answer: 1000

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

QUESTION 14:

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

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

Correct Answer: c

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

The correct option is (c).

QUESTION 15:

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

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

Correct Answer: c

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

Thus, the correct option is (c).

QUESTION 16:

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

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

Correct Answer: c

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

The correct option is (c).

QUESTION 17:

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

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

Correct Answer: a, b, c

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

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

QUESTION 18:

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

a. True
b. False

Correct Answer: a

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

QUESTION 19:

Can the use of firewall prevent port/host scanning?

a. True
b. False

Correct Answer: a

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

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