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. Hypervisor allows one host system to support multiple virtual machines by sharing the resources.
b. Hypervisor allows one host system to support multiple virtual machines; however, it does not allow resource sharing.
c. Kali-linux is a Debian-based Linux distribution that has collection of tools that are useful for penetration testing.
d. Kali-linux is a hack-proof secured operating system.
e. None of these.

Correct Answer: a, 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; 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. No systems can be considered as hack-proof.

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

QUESTION 2:

Which of the following statement(s) is/are **true** about "Active 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: b, c

Detailed Solution: Reconnaissance is the process of gathering information about a target network or system. 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 (b) and (c).

QUESTION 3:

Which of the following information **cannot** be retrieved using Whois database lookup?

a. Registration details
b. Name Servers.
c. IP Address
d. History of the website.
e. None of these.

Correct Answer: d

Detailed Solution: Using Whois database lookup we can retrieve various useful information about the target system, such as IP address, registration details, mail id, contact, name servers, domain owner, etc. However, we cannot retrieve history of the website. To check complete history of the website, archive.org can be used.

Thus the correct option is (d).

QUESTION 4:

What is the main objective of port scan?

a. Identification of live hosts.
b. Identification of services running in the target system.
c. Identification of the operating system of the target systems.
d. None of these.

Correct Answer: b

Detailed Solution: Port in a system tells us about the services running in the target machine, i.e. if port 80 is used for http, port 443 is used for https, etc. Thus, the main objective of port scanning is to identify the services running in the target system.

The correct option is (b).

QUESTION 5:

Which of the following statement(s) is/are **true** for host discovery using ICMP ECHO sweep?

a. For ICMP ECHO sweep; -PP option is used.
b. The attacker sends out an ICMP ECHO request packet to the target, and waits for an ICMP ECHO reply response.
c. If the attacker does not receive an ICMP ECHO reply then the host is considered as down.
d. If the attacker does not receive an ICMP ECHO reply then the host is considered as live.

Correct Answer: b, c

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. In Non-Echo ICMP sweep, ICMP time stamp and ICMP mask request packet are used. To perform ICMP ECHO sweep – PE option is used.

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

QUESTION 6:

Which of the following options are used for host discovery using TCP and UDP sweep respectively?

a. PE, PA
b. PP, PU
c. PM, PA
d. PA, PU

Correct Answer: d

Detailed Solution: PE option is used for ICMP Echo sweep. PM and PP options are used for ICMP Non-Echo sweep. PS and PA option are used for TCP sweep and PU is used for UDP sweep.

Thus correct option is (d).

QUESTION 7:

Which of the following option is used for OS detection?

a. PO
b. Os

c. O
d. sO
e. None of these.

Correct Answer: c

Detailed Solution: for OS detection -O option is used. OS and version can also be scanned using only –A option 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 8:

How many ports are scanned in NMAP for a target system if we use –F option _____?

Correct Answer: 100

Detailed Solution: -F option limits the port scanning to top 100 ports.

QUESTION 9:

If we want to disable host discovery in port scanning, then which of the following options can be used?

a. F
b. p
c. Pn
d. sn
e. We cannot disable host discovery.

Correct Answer: c

Detail Solution: The Pn options tells nmap not to carry out host discovery and consider all host as up and start port scanning.

Thus the correct option is (c).

QUESTION 10:

Which of the following can be used to reconnaissance countermeasures?

a. Do not release critical info in public.
b. Encrypt password and sensitive information.

c. Restrict zone transfer.
d. Examine logs periodically.
e. Use firewalls.

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

Detail Solution: All of the given options can be used for reconnaissance countermeasures.

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