Course Name: ETHICAL HACKING

Assignment- Week 5

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

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

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

Correct Answer: b, d

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

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

QUESTION 2:

Which of the following may be used for password cracking?

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

Correct Answer: a, b

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

QUESTION 3:

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

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

Correct Answer: a

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

The correct option is (a).

QUESTION 4:

Which of the following can self-replicate itself?

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

Correct Answer: b

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

The correct option is (b).

QUESTION 5:

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

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

Correct Answer: a, b, c, d

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

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

QUESTION 6:

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

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

c. nmap -- script script_name

d. nmap script_name.nse

Correct Answer: a, b, c

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

QUESTION 7:

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

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

Correct Answer: a

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

The correct option is (a).

QUESTION 8:

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

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

Correct Answer: a, b, c

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

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

QUESTION 9:

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

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

Correct Answer: a, d

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

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

QUESTION 10:

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

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

Correct Answer: a, d

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

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

QUESTION 11:

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

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

Correct Answer: a

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

The correct option is (a).

QUESTION 12:

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

a. Client
b. Server

Correct Answer: b

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

The correct option is (b).

QUESTION 13:

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

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

Correct Answer: d

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

The correct option is (d).

QUESTION 14:

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

a. True

b. False

Correct Answer: a

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

The correct option is (a).

QUESTION 15:

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

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

Correct Answer: a

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

The correct option is (a).

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