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: 12 **Total mark: 12 x 1 = 12**

QUESTION 1:

Which of the following NMAP options can be used to run some of the nmap scripts?

a. PE
b. PU
c. A
d. O
e. sC

Correct Answer: c, e

Detail Solution: sC performs a script scan using the default set of scripts. It is equivalent to --script=default. Option "A" which is known as aggressive scan enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute).

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

QUESTION 2:

Which of the following NMAP scripts is used to perform DoS attack?

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

Correct Answer: e

Detail Solution: -ssh-brute is used to crack credential of ssh service; smb-brute is used to crack user credential; smb-os-discovery is used to identify the OS of the target system; 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-dos-attack.

The correct option is (e).

QUESTION 3:

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

a. Nessus
b. Hydra
c. crunch
d. hascat
e. NMAP

Correct Answer: a, e

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

Hydra is used for password cracking, crunch is used for making dictionary, hascat is used to generate has passwords.

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

QUESTION 4:

Which of the following tools can be used to create a dictionary for dictionary-based password attack?

a. Hydra
b. Crunch
c. SQLMAP
d. None of these.

Correct Answer: b

Detail Solution: To create a dictionary Crunch tool can be used. Hydra is used for dictionary based password attack. SQLMAP is use for sql injection attacks.

Thus the correct option is (b).

QUESTION 5:

Consider the following statements:

(i) User enumeration refers to collecting details of users and their privileges.

(ii) Hydra and Crunch tool can be used for user enumeration.

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: User enumeration refers to collecting details of user and there privilege. It can also give details for password rules, however it cannot generate password for respective users. For enumeration we can use tools such as enum4linux, rpcclient. We can also use an nmap scrip smb-enum-users for user enumeration. Hydra and Crunch are used for password cracking.

Thus the correct option is (a).

QUESTION 6:

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

Correct Answer: b, c

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.

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

QUESTION 7:

How many words will be generate by crunch tool if we use the crunch command as “**crunch 1 2 0123456789**” ?

Correct Answer: 110

Detail Solution: The given command will generate word list with only numbers of length 1 and 2.

So in total the command will generate (100 words 0-99 and 00 to 09) = 110 words.

QUESTION 8:

Which of the following can be used for gaining same level privilege as the existing one?

a. Vertical privilege escalation.

b. Horizontal privilege escalation.

c. Diagonal privilege escalation.

d. Triangular privilege escalation.

e. None of these.

Correct Answer: b

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.

The correct option is (b).

QUESTION 9:

Which of the following tools can be used for user enumeration?

a. Hydra

b. Crunch

c. Enum4linux

d. None of these.

Correct Answer: c

Detail Solution: 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 option is (c).

QUESTION 10:

To download any file from the target system that is connected through FTP connection, which of the following commands can be used?

a. put

b. get

c. upload

d. download

Correct Answer: b

Detail Solution: To upload any file we use the “put” command. To download a file “get” command is used.

The correct option is (b).

QUESTION 11:

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

a. Malware are malicious software that damages or disables computer systems and gives limited or full control to the malware creator for the purpose of theft or fraud.

b. Malware can get inside systems through file sharing or fake programs.

c. Malwares can alter, corrupt, modify or delete some data/files.

d. None of these.

Correct Answer: d

Detail Solution: Malwares are malicious softwares that damage or disable computer systems and give limited or full control to the malware creator for the purpose of theft or fraud. It can modify or delete data/files. Malware are used to get inside system using file sharing or by fake software. All the given statements are true.

The correct option is (d).

QUESTION 12:

Which of the following commands is used to delete an ARP entry?

a. arp -l
b. arp -s
c. arp -i
d. arp –e
e. None of these

Correct Answer: e

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 (e).

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