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: **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
e. Crunch

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. Hypervisor is a software tool used for virtualization. Hydra and Crunch are used for performing password attack.

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

QUESTION 2:

NMAP scripts can be used for:

a. Vulnerability scanning
b. Backdoor detection.
c. Port detection.
d. Password attack.
e. None of these.

Correct Answer: a, b, c, d

Detail Solution: The NMAP scripts can be useful for automated scanning. NMAP scripts can be used for vulnerability detection, backdoor detection, port detection, performing password attacks etc.

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

QUESTION 3:

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

a. smb-os-brute
b. smb-os-discovery
c. http-os-check
d. None of these.

Correct Answer: b

Detail Solution: smb-os-discovery is used to identify the OS of the target system; there is no script such as smo-os-brute, http-os-check.

Thus the correct option is (b).

QUESTION 4:

Which of the following scripts can be used to detect if a target system is vulnerable to DoS attack?

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

Correct Answer: d

Detail Solution: http-methos script is used to check if the host is running a web server on particular port. It can also identify 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. There is no script named as http-dos-check.

The correct option is (d).

QUESTION 5:

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

Correct Answer: 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. None of the commands are correct.

Thus the correct option is (d).

QUESTION 6:

The necessary parameters required to generate word list using crunch tool is:

a. Minimum length of the word list.
b. Maximum length of the word list.
c. File name where the word list will be stored.
d. No parameters are required to generate a word list.

Correct Answer: a, b

Detail Solution: To generate a word list using crunch, the necessary parameters which needs to be provided are minimum and maximum length of the word list. All other parameters are optional.

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

QUESTION 7:

Which of the following tools can be used to perform password attack?

a. Hydra
b. Archive.org
c. Netcraft
d. Whois
e. None of these.

Correct Answer: a

Detail Solution: To perform password attack we can use Hydra tool.

Thus the correct option is (a).

QUESTION 8:

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. Triangular privilege escalation.
e. 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/triangular privilege escalation.

Thus the correct option is (a).

QUESTION 9:

Which of the following approaches can be used to extract information about all users 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 10:

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 11:

To upload any file in the target system which is connected through FTP connection which of the following command can be used?

a. put
b. get
c. upload
d. download

Correct Answer: a

Detail Solution: To upload any file we use the "put" command.

The correct option is (a).

QUESTION 12:

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 13:

How a malware can get inside into a system?

a. Removable devices
b. Attachments
c. Fake Programs
d. Untrusted sites and freeware software.

Correct Answer: a, b, c, d

Detail Solution: Malware can get inside the system through all the given approaches.

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 all arp entries 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*******