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 0.8 = 12**

QUESTION 1:

Consider the following statements:

(i) The purpose of vulnerability scanning is to identify weakness of system/network in order to determine how a system can be exploited.

(ii) NMAP script can be useful for automated scanning. However, scripts can have specific requirement.

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: c

Detail Solution: The purpose of vulnerability scanning is to identify vulnerabilities and weaknesses of a system/network in order to determine how a system can be exploited. Typical tools that are used for scanning vulnerabilities in hosts and networks are NMAP, Nessus, Nexpose, MPSA, etc. NMAP scripts can be useful for automated scanning, however each script can have specific requirement, i.e. some specific ports should be open on the target system.

Thus the correct option is (c).

QUESTION 2:

Which of the following NMAP option runs some of the nmap scripts?

a. -A
b. -sC
c. -pn
d. -PE
e. –sL

Correct Answer: a, b

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

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

QUESTION 3:

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

a. ssh-brute
b. smb-os-discovery
c. smb-brute
d. http-slowloris-check
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.

Thus the correct options is (e).

QUESTION 4:

Which of the following tools/software **cannot** be used for scanning vulnerabilities?

a. Hypervisor
b. Nessus
c. Hydra
d. crunch
e. hascat
f. Nmap

Correct Answer: a, c, d, e

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

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

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

QUESTION 5:

Which of the following tool/approach can be used for proxy preparation?

a. Web based proxy/Proxychains tools
b. By running NMAP vulnerability scanning scripts.
c. Macchanger tool
d. Hypervisor
e. Firewall

Correct Answer: a, c

Detail Solution: For proxy preparation, we can use web based proxy or Proxychains tools to change our IP. To change mac address we can use macchanger tool.

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

QUESTION 6:

Which of the following is **not** a password cracking approach?

a. Shoulder Surfing
b. Social Engineering
c. Dictionary Attack
d. Brute-Force attack
e. Rule Based Attack
f. None of these.

Correct Answer: f

Detail Solution: All of the approach can be used for password cracking. In Shoulder Surfing attacker spy at the user's keyboard or screen while he/she is logging in. In Social Engineering attack, attacker convince victim to reveal passwords. In Dictionary Attack a dictionary file is used that runs against user accounts. In Brute-Force Attack, attacker tries, every combination of characters until the password is broken. Rule-based Attack is used when the attacker gets some information about the password.

Thus the correct option is (f).

QUESTION 7:

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

a. Hydra

b. Crunch
c. Nessus
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. Nessus is used for vulnerability scanning.

Thus the correct option is (b).

QUESTION 8:

Which of the following statement(s) is/are **true** for user enumeration?

a. Enumeration refers to collecting details of users and their privileges.
b. User enumeration refers to collecting username and passwords.
c. NMAP does not have any script for user enumeration.
d. Hydra and crunch tool can be used for user enumeration.

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. However, hydra and crunch is used for password cracking.

Thus the correct option is (a).

QUESTION 9:

Which of the following can be used for gaining same level 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: 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.

Thus the correct option is (b).

QUESTION 10:

Which of the following approaches can be helpful to avoid privilege escalation attack?

a. Run user level application on least privileges.
b. Keep the software updated.
c. Regularly perform vulnerability scan.
d. Institute a strong password policy.
e. Avoid downloading files from untrusted/malicious websites.
f. Ignore unknown mails.

Correct Answer: a, b, c, d

Detail Solution: The approach given in option a, b, c, d can be useful for avoiding privilege escalation. The approach given in option e and f can be helpful against malware/social engineering attack.

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

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. Malware cannot replicate itself.
d. Malwares can alter, corrupt, modify or delete some data/files.
e. None of these.

Correct Answer: c

Detail Solution: 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. It can modify or delete data/files. Malware are usually get inside system using file sharing or by fake software. Some specific type of malwares such as virus and worms typically replicate themselves and get attached to other files.

The correct option is (c).

QUESTION 12:

Which of the following can be used as a countermeasure against malwares?

a. Use of firewall
b. Avoid downloading files from untrusted/malicious websites
c. Use of antivirus tools
d. Keep computer and software updated.
e. Ignoring unknown mails
f. All of these

Correct Answer: f

Detail Solution: All of the given approaches can be used as a countermeasure against Malwares.

QUESTION 13:

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

a. Sniffing is a process of monitoring and capturing all data packets passing through a given network.
b. The HTTPS packets are vulnerable to sniffing attack.
c. In passive sniffing ARP packets are used to flood the switch's CAM table.
d. None of these.

Correct Answer: b, c

Detail Solution: Sniffing is a process of monitoring and capturing all data packets passing through a given network. Sniffing is categorized into two types: active and passive. In passive sniffing, sniffing is done on a hub where traffic is sent to all device. Passive sniffing involves only monitoring. Active sniffing is used against switch-based network. In active sniffing first the switch CAM table is flooded with incorrect ARP entries. Mostly the unsecured protocols which shares data in plaintext are vulnerable to sniffing.

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

QUESTION 14:

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

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).

QUESTION 15:

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

a. ARP spoofing involve construction of large number of forged ARP request/reply packets.

b. Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.

c. In MAC attack, CAM table are flooded with fake MAC address and IP pairs.

d. MAC attack cannot change the behavior of the switch.

e. MAC attack can fill the CAM table of adjacent switches.

f. None of these.

Correct Answer: a, b, c, e

Detail Solution: ARP spoofing involve construction of large number of forged ARP request/reply packets. Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC. In MAC attack, CAM table are flooded with fake MAC address and IP pairs. MAC attack can change the behavior of switch to act like a hub and can also fill the CAM table of adjacent switch.

Thus the true options are (a), (b), (c) and (e).

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