Course Name: ETHICAL HACKING

Assignment- Week 12

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 8 x 1.25 = 10**

QUESTION 1:

NMAP command can be used for?

a. Host Discovery
b. Port Scanning
c. Service and Version Detection
d. OS Detection
e. Vulnerability Scanning

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

Detail Solution: NMAP can perform all of the above operations. Along with this we can also perform brute force attack using NMAP scripts.

QUESTION 2:

In UDP sweep scan, a scanner sends a UDP datagram and receives an ICMP port unreachable message from target. What does it indicates?

a. Target is alive/up
b. Target is down.

Correct Answer: a

Detail Solution: If the sender receives ICMP port unreachable packet this indicates that the target is up. The correct option is (a).

QUESTION 3:

Which NMAP options can be used for UDP sweep scan?

a. -PS

b. -PU
c. –sU
d. -PE
e. None of these.

Correct Answer: b, c

Detail Solution: UDP sweep is carried out using the –PU or –sU option in NMAP. Hence, the correct answers are (b) and (c).

QUESTION 4:

How many host (IP) will be scanned by following NMAP command?

```
nmap –sL 192.168.62.48/24
```

a. 256
b. 1024
c. 24
d. 2

Correct Answer: a

Detail Solution: The given command will scan all hosts with IP addresses 192.168.62.0 to 192.168.62.255

Thus, a total of 256 IP addresses will be scanned. The correct option is (a).

QUESTION 5:

Consider the following statements and answers.

(i) An open port indicates that some application is running on the target system on that particular port.

(ii) A filtered port indicates that either the firewall or any other filter software is blocking nmap request.

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: An Open port indicates that some service are running on the port and nmap can identify this, a filtered port indicates that nmap cannot access that as some filtering software is blocking the nmap request.

Thus, both statements (i) and (ii) are correct.

QUESTION 6:

By default how many ports are scanned using –F and –p option respectively?

a. 100, 1000
b. 1000, 100
c. 65536, 65536
d. None of these.

Correct Answer: a

Detail Solution: -F and –p option scans top 100 and 1000 ports respectively.

Thus, the correct option is (a).

QUESTION 7:

Which of the following NMAP commands are valid?

a. nmap 192.168.62.43
b. nmap www.nptel.ac.in
c. nmap 192.168.62.43-48
d. nmap 192.168.62.43,44,45

Correct Answer: a, b, c, d

Detail Solution: All the given nmap commands are valid.

QUESTION 8:

Which of the following statement(s) is/are false for sniffing tools like Wireshark/Burpsuite?

a. They can capture packets from almost all network protocols like TCP, IP.
b. Some sniffing tools support packet manipulation.

c. Some sniffing tools can also be used for scanning vulnerabilities in web applications.
d. None of these.

Correct Answer: d

Detail Solution: Sniffing tools can capture packets from almost all the known network protocols, some sniffing tools can be used for packet manipulation and vulnerability scanning, viz. burp suite.

The correct option is (d).

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

Course Name: ETHICAL HACKING

Assignment Solution- Week 11

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following Metasploit module can be used for vulnerability scanning and brute force attack?

a. Encoder
b. Payload
c. Exploit
d. Auxiliary

Correct Answer: d

Detail Solution: Encoder module is used to encode the payloads. Exploit module is used to take advantage of System/Application bugs. Payload module is used to establish communication channel between Metasploit framework and target system. Auxiliary module is used to perform brute force attack, DoS attack, host and port scanning, vulnerability scanning, etc.

The correct option is (d).

QUESTION 2:

To set port number of the target system in Metasploit framework, which of the following commands is used?

a. Set LHOST
b. Set RHOST
c. Set RPORT
d. Set LPORT

Correct Answer: c

Detail Solution: LHOST and RHOST options are used to set IP of local and target (remote) system, whereas LPORT and RPORT are used to set port number for local and target system.

The correct option is (c).

QUESTION 3:

What of the following is/are true for meterpreter shell?

a. An interactive command shell (terminal) that helps to explore target system.
b. A standard command shell (terminal) that helps to explore target system.
c. We can use Metasploit modules and commands inside meterpreter shell.
d. We cannot use Metasploit modules and command inside meterpreter shell.

Correct Answer: a, c

Detail Solution: A Meterpreter shell gives access to Metasploit modules and other actions not available in the standard command shell.

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

____

QUESTION 4:

Which of the following commands can be used for privilege escalation in Metasploit framework?

a. getuid
b. getsystem
c. hashdump
d. ps

Correct Answer: b

Detail Solution: getuid is used to get user id. getsystem is used to escalate privilege and get administrative login. hashdump is used to get user account details, and ps is used to get details of all running process of the target system.

The correct option is (b).

____

QUESTION 5:

To create a payload (backdoor), which parameters needs to be set in msfvenom module?

a. Name of the payload
b. IP of the target system
c. IP of an attacker system
d. Port of target system

e. Port of an attacker system.

Correct Answer: a, c, e

Detail Solution: To create payload, name of payload, IP and port of the attacker system are required.

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

QUESTION 6:

Consider the table "USERS" consist of 3 column u_id, u_name and pass as given below:

u_id	u_name	pass
1	NPTEL	nptel1234
2	IIT_KGP	kgp1234
3	Eth_Hack	eth4321

Which of the following SQL queries are malicious with respect to the above table?

a. SELECT * from USERS;
b. SELECT * from USERS where u_id = "5"
c. SELECT * from USERS where u_name = "any"
d. SELECT * from USERS where u_name = "any" or 1=1

Correct Answer: d

Detail Solution: The first three SQL queries are valid queries, however, we will not get any output for the queries (b) and (c). The last query is a malicious query, which have the malicious condition 1=1.

The correct option is (d).

QUESTION 7:

If any web page is vulnerable to blind sql injection then which of the following is true?

a. It will print error message for incorrect user input.
b. It will not print anything for incorrect user input.

Correct Answer: b

Detail Solution: If the webpage is vulnerable to blind sql injection then it will not generate any output (no error message).

The correct option is (b).

QUESTION 8:

Which of the following tools is used to automate sql injection attacks?

a. Accunetix
b. Metasploit
c. SQL MAP
d. NMAP

Correct Answer: c

Detail Solution: To automate sql injection attack, SQL MAP tool can be used. NMAP and Accunetix are used for vulnerability scanning in a network or web application, whereas Metasploit framework is used to exploit various weakness of the system.

The correct option is (c).

QUESTION 9:

Which of the following options can be used to extract the current user name in SQL MAP?

a. - - users
b. - - current-user
c. - - current-db
d. - - dbs

Correct Answer: b

Detail Solution: --current-user option is used to get the current user name in SQL MAP.

The correct option is (b).

QUESTION 10:

Which of the following statement(s) is/are true for reflected XXS?

a. It affects all users of that web application.
b. It affects only a single client of the web application.
c. It is stored in the database of web application.
d. None of these.

Correct Answer: b

Detail Solution: Stored XSS are stored in database of web application and can affect all users; however, reflected XSS is limited to a single client.

The correct option is (b).

____

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

Course Name: ETHICAL HACKING

Assignment- Week 10

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following are examples of hardware-based attacks?

a. Side-channel attack.
b. Physical probing.
c. Denial of service stack.
d. SQL injection attack

Correct Answer: a, b

Detail Solution: In side-channel attack, some side channels (like delay, power, etc.) are monitored during some computation using some sophisticated measuring instruments, and as such requires access to the hardware that runs the computation. In comparison, denial-of-service and SQL injection are essentially software-based attacks.

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

QUESTION 2:

Which of the following statement(s) is/are false for side channel attacks?

a. They exploit weaknesses in cryptographic algorithms.
b. They exploit weaknesses in algorithm implementations.
c. They do not require physical access to the device.
d. None of these.

Correct Answer: a, c

Detail Solution: Side-channel attacks basically exploit weaknesses in the implementation (hardware or software) of an algorithm. It requires physical access to the device for measurement of some parameter. They are not dependent on the weaknesses of the algorithm.

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

QUESTION 3:

Which of the following are typically exploited in side-channel attacks?

a. Time required to carry out some computation.
b. Encrypted ciphertexts for a number of given plaintext messages.
c. Birthday attack of the hash function used.
d. Variation in power consumption during computation.
e. All of these

Correct Answer: a, d

Detail Solution: Timing and power analysis attacks are very common in mounting side-channel attacks. It does not rely on analysis of ciphertexts or mounting birthday attack on hash functions.

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

QUESTION 4:

For modular exponentiation computation of x^{25}, how many squaring and multiplication operations would be required?

a. 4 and 4.
b. 4 and 2.
c. 3 and 4.
d. 5 and 2.
e. 5 and 3.

Correct Answer: b

Detail Solution: The binary representation of 25 is 11001.

Thus, $x^{25} = x^{16} * x^{8} * x^{1} = (x^{8} * x^{4})^{2} * x^{1} = ((x^{4} * x^{2})^{2})^{2} * x^{1} = (((x^{2} * x)^{2})^{2})^{2} * x^{1}$

This computation requires 4 squarings and 2 multiplication operations.

The correct option is (b).

QUESTION 5:

Which of the following is/are true for differential power analysis?

a. It requires a single measurement.
b. It requires multiple measurements.
c. It is more effective than simple power analysis.
d. It is less effective than simple power analysis.

Correct Answer: b, c

Detail Solution: Differential power analysis is more sophisticated and effective as compared to simple power analysis. Differential power analysis requires multiple measurements.. The correct options are (b) and (c).

QUESTION 6:

Which of the following can prevent power analysis attacks?

a. The computation times in the different branches of an "if" statement must be unequal.
b. The computation times in the different branches of an "if" statement must be the same.
c. Package the chip in a tamper-proof casing.
d. All of these.

Correct Answer: b

Detail Solution: Power analysis attack can be prevented by making all the branches in conditional statements symmetric with respect to computation. It does not require breaking the casing of the chip. The correct option is (b).

QUESTION 7:

What is the full form of PUF?

a. Perfect Unitary Function
b. Preset Until Fail.
c. Physically Undefined Function.
d. None of these.

Correct Answer: d

Detail Solution: The full form of PUF is Physically Unclonable Function. The correct option is (d).

QUESTION 8:

Which of the following is/are true for a PUF?

a. Physical properties of a device are used to generate a key, which is different from one manufactured device to the next.
b. The key is stored on-chip and is well protected.
c. The key obtained from the PUF can be modified as required.
d. None of these.

Correct Answer: a

Detail Solution: In a PUF, the key is generated exploiting the uniqueness in the challenge-response pairs of a device. The key is not stored anywhere in the device. The key as generated depends on device characteristics and cannot be changed. The correct option is (a).

QUESTION 9:

What is a hardware Trojan?

a. It is a form of PUF that can be used for attacking.
b. It is a malicious modification of the circuitry in a chip.
c. It is a form of PUF that is used for preventing attacks.
d. None of these.

Correct Answer: b

Detail Solution: A hardware Trojan is not a PUF. It refers to some malicious modification to the hardware, such that whenever some triggering condition becomes true, some unintended operation (called payload) is activated. The correct option is (b).

QUESTION 10:

Which of the following types of PUF can be used?

a. Ring oscillator PUF.
b. SRAM PUF.
c. FPGA PUF.
d. Programmable PUF.

Correct Answer: a, b

Detail Solution: Ring oscillator PUF and SRAM PUF are two types of PUF that can be used. The correct options are (a) and (b).

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