Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Engineering

End Sem (Even) Examination May-2022

CS3EY05 Ethical Hacking

Programme: B.Tech. Branch/Specialisation: CSE

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. What port number does HTTPS use? 1

(a) 53 (b) 443 (c) 80 (d) 21

ii. Someone has breached a website and managed to keep it a secret. The hack was not part of an assignment and there was no permission. What is this process called___? 1

(a) Black hat hacker (b) Hacktivist

(c) Scriptkiddle (d) White hat hacker

iii. What is the attack called 'evil twin'? 1

(a) Rogue access point (b) ARP poisoning

(c) Session hijacking (d) MAC spoofing

iv. Which of the following is a passive wireless discovery tool? 1

(a) Kismet (b) Netsniff

(c) Aircrack (d) NetStumbler

v. Which of the following is not a web server attack type? 1

(a) DOS attack

(b) Directory Traversal

(c) Website Defacement using SQLi

(d) Password guessing

vi. _____ is any action that might compromise cyber security. 1

(a) Threat (b) Vulnerability

(c) Exploit (d) Attack

vii. Which of the following attacks would compromise the integrity of system information? 1

(a) Denial-of-service (b) Smurf

(c) SQL Injection (d) Fraggle

P.T.O.

viii. The Information Technology Act 2000 is an Act of Indian Parliament notified on- **1**
(a) 27th October 2000 (b)15th December 2000
(c) 17th November 2000 (d)17th October 2000

ix. Assessing Computer without prior authorization is a cybercrime that comes under____. **1**
(a) Section 65 (b) Section 66 (c) Section 68 (d) Section 70

x. What is the maximum length of an SSID? **1**
(a) Thirty-two characters (b) Sixteen characters
(c) Sixty-four characters (d) Eight characters

Q.2 i. What are the best defenses against a brute force login attack? **2**

ii. Define the followings: **3**
(a) White Hat Hacker (b) Black Hat Hacker
(c) Grey Hat Hacker

iii. List out the phases of Ethical Hacking & required tools. **5**

OR iv. What do you mean by common cyber-attack? List out any three of them. **5**

Q.3 i. Explain Session Hijacking. **2**

ii. Define the following: **8**
(a) Hash Injection attack (b) Rainbow table attack

OR iii. Define the following with a suitable example: **8**
(a) Spoofing (b) Distributed network attack

Q.4 i. What do you mean by SQL Injection? How one can prevent it? **3**

ii. How does social engineering work? List out some popular types of social engineering and explain them in brief. **7**

OR iii. Define Honeypot and explain how it is useful to catch hacker. **7**

Q.5 i. What is the requirement for low level reporting & high-level reporting of penetration testing result? Define it in detail. **4**

ii. What is report writing? List out its phases. **6**

OR iii. What metrics are included in CVSS to evaluate a vulnerability? How it is useful in vulnerability scoring? **6**

Q.6 Attempt any two:

i. List out the steps to file a complaint of suspected hacking. **5**

ii. List out the salient features of Information Technology Act-2000. **5**

iii. What do you mean by hacker vs cracker liabilities? **5**

******

Marking Scheme
CS3EY05 Ethical Hacking

Q.1	i.	What port number does HTTPS use? (b) 443		1
	ii.	Someone has breached a website and managed to keep it a secret. The hack was not part of an assignment and there was no permission. What is this process called___? (b) Hacktivist		1
	iii.	What is the attack called 'evil twin'? (a) Rogue access point		1
	iv.	Which of the following is a passive wireless discovery tool? (a) Kismet		1
	v.	Which of the following is not a web server attack type? (d) Password guessing		1
	vi.	_____ is any action that might compromise cyber security. (a) Threat		1
	vii.	Which of the following attacks would compromise the integrity of system information? (c) SQL Injection		1
	viii.	The Information Technology Act 2000 is an Act of Indian Parliament notified on- (d)17th October 2000		**1**
	ix.	Assessing Computer without prior authorization is a cybercrime that comes under____. (b) Section 66		**1**
	x.	What is the maximum length of an SSID? (a) Thirty-two characters		**1**
Q.2	i.	Any two point	1 Mark each (1 Mark*2)	**2**
	ii.	(a) White Hat Hacker (b) Black Hat Hacker (c) Grey Hat Hacker	1 Mark 1 Mark 1 Mark	**3**
	iii.	List out the phases of Ethical Hacking (3 phases) Required tools.	3 Marks 2 Marks	**5**
OR	iv.	Common cyber-attack List out any three of them.	2 Marks 1 Mark each (1 Mark*3)	**5**
Q.3	i.	Session Hijacking.	2 Marks	**2**
	ii.	(a) Hash Injection attack (b) Rainbow table attack	4 Marks 4 Marks	**8**
OR	iii.	(a) Spoofing (b) Distributed network attack	4 Marks 4 Marks	**8**
Q.4	i.	What do you mean by SQL Injection How one can prevent it	2 Marks 1 Mark	**3**
	ii.	How does social engineering work List out some popular types of social engineering Explain them in brief.	3 Mark 1 Mark 3 Marks	**7**
OR	iii.	Define Honeypot Diagram of Honeypot Explain how it is useful to catch hacker.	2 Marks 2 Marks 3 Marks	**7**
Q.5	i.	Low level reporting High-level reporting	2 Marks 2 Marks	**4**
	ii.	What is report writing List out its phases.	2 Marks 4 Marks	**6**
OR	iii.	Definition of CVSS Metrics included Vulnerability scoring	2 Marks 2 Marks 2 Marks	**6**
Q.6		Attempt any two:		
	i.	Five steps	1 Mark each (1 Mark*5)	**5**
	ii.	Five features	1 Mark each (1 Mark*5)	**5**
	iii.	What do you mean by hacker vs cracker liabilities?	2.5 Marks 2.5 Marks	**5**

******