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

Enrollment No......................................

Faculty of Engineering
End Sem Examination May-2023
CS3EY05 Ethical Hacking

Programme: B.Tech. Branch/Specialisation: CSE / All

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. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. In reverse engineering process, what refers to the sophistication of the design information that can be extracted from the source code? **1**

(a) Interactivity (b) Completeness
(c) Abstraction level (d) Direction level

ii. ______ is a weakness that can be exploited by attackers. **1**

(a) System with virus
(b) System without firewall
(c) System with vulnerabilities
(d) System with a strong password

iii. ______ attack is the exploitation of the web-session & its mechanism that is usually managed with a session token. **1**

(a) Session hacking (b) Session hijacking
(c) Session cracking (d) Session compromising

iv. Password cracking in system hacking is of ______ types. **1**

(a) 2 (b) 3 (c) 4 (d) 5

v. Point out the correct statement- **1**

(a) Parameterized data cannot be manipulated by a skilled and determined attacker
(b) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities
(c) The primary form of SQL injection consists of indirect insertion of code
(d) None of these

P.T.O.

vi. What is the purpose of a shadow honeypot? **1**

(a) To flag attacks against known vulnerabilities

(b) To help reduce false positives in a signature-based IDS

(c) To randomly check suspicious traffic identified by an anomaly detection system

(d) To enhance the accuracy of a traditional honeypot

vii. The two commonly used penetration tests are ______. **1**

(a) Standard penetration test (b) Cone penetration test

(c) Both (a) & (b) (d) None of these

viii. On which is the National Vulnerability database primarily build upon ______. **1**

(a) Vulnerabilities (b) NVD

(c) Patch (d) CVE Identifiers

ix. Under which section of IT act, stealing any digital asset or information is written a cybercrime? **1**

(a) 65 (b) 65-D (c) 67 (d) 70

x. Who is the father of computer security? **1**

(a) August Kerckhoffs (b) Bob Thomas

(c) Robert (d) Charles

Q.2 i. Explain the phases of ethical hacking. **2**

ii. Discuss ethical hacking. Why is it necessary? **3**

iii. Write short note on: **5**

(a) White hat hacker (b) Black hat hacker

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

Q.3 i. Discuss ethical hacking of web servers. **4**

ii. Write short note on: **6**

(a) Password cracking (b) Hash injection

OR iii. Write short note on: **6**

(a) Replay and man-in-the-middle attacks

(b) Rainbow table attack

(c) Distributed network attack

Q. 4 i. Define type of scanning – TCP SYN, ACK, XMAS & UDP. **3**

ii. Describe hacking wireless networking and hacking mobile platforms. **7**

OR iii. What do you understand by social engineering? List out some popular types of social engineering and explain them in brief. **7**

Q.5 i. What are mitigation of issues identified including tracking? **2**

ii. Elaborate CVSS scoring for vulnerabilities. **3**

iii. What is report writing? List out its phases. **5**

OR iv. Write short note on requirements for low level reporting & high-level reporting of penetration testing. **5**

Q.6 Attempt any two:

i. Write a short note on India's information technology amendment act 2008. **5**

ii. Differentiate between hacker vs cracker, liabilities. **5**

iii. Explain how hacking is legally dealt with among BRICS countries. **5**

******

Marking Scheme
CS3EY05[T]- Ethical Hacking

Q.1 i) In reverse engineering process, what refers to the sophistication of the design information that can be extracted from the source code? 1

c) abstraction level

ii) ___________ is a weakness that can be exploited by attackers. 1

c) System with vulnerabilities

iii) _____________ attack is the exploitation of the web-session & its mechanism that is usually managed with a session token. 1

b) Session Hijacking

iv) Password cracking in system hacking is of ________ types. 1

c) 4

v) Point out the correct statement. 1

b) Procedure that constructs SQL statements should be reviewed for injection vulnerabilities

vi) What is the purpose of a shadow honeypot? 1

c) To randomly check suspicious traffic identified by an anomaly detection system

vii) The two commonly used penetration tests are 1

c) Both (a) & (b)

viii) On which is the National Vulnerability database primarily build upon......... 1

d) CVE Identifiers

ix) Under which section of IT act, stealing any digital asset or information is written a cyber crime? 1

a) 65

x) Who is the father of computer security? 1

a) August Kerckhoffs

Q.2 i. Explain the phases of ethical hacking. **(two phases 2 marks)** 3

ii. Discuss Ethical Hacking. **(1.5 marks)** Why is it necessary?**(1.5 marks)** 2

iii. Write short note on: 5

a) White Hat Hacker **(2.5 marks)**

b) Black Hat Hacker **(2.5 marks)**

OR iv. What do you mean by common cyber-attack? **(2 marks)** List out any three of them. **(3 marks)** 5

Q.3 i. Discuss ethical hacking of Web Servers. **(4 marks)** 4

ii. Write short note on: 6

a) Password Cracking **(3 marks)**

b) Hash Injection **(3 marks)**

OR iii. Write short note on: 6

a) replay and man-in-the-middle attacks **(2 marks)**

b) rainbow table attack **(2 marks)**

c) distributed network attack **(2 marks)**

Q. 4 i. Define type of scanning – TCP SYN, ACK, XMAS & UDP. **(1 mark each)** 3

ii. Describe Hacking Wireless Networking **(4 marks)** and Hacking mobile platforms **(3 marks)**. 7

OR iii. What do you understand by social engineering? **(2 marks)** List out some popular types of social engineering **(2 marks)** and explain them in brief. **(3 marks)** 7

Q.5 i. What are mitigation of issues identified including tracking? **(2 marks)** 2

ii. Elaborate CVSS scoring for vulnerabilities. **(3 marks)** 3

iii. What is report writing? **(2.5 marks)** List out its phases. **(2.5 marks)** 5

OR iv. Write short note on requirements for low level reporting **(2.5 marks)** & high-level reporting of Penetration testing. **(2.5 marks)** 5

Q.6 Attempt any two:

i. Write a short note on India's Information Technology Amendment Act 2008. **(4 marks)** 5

ii. Differentiate between hacker liabilities **(3 marks)** vs cracker liabilities. **(3 marks)** 5

OR iii. Explain how hacking is legally dealt with among BRICS countries. (**Pointwise explaination 6 marks)** 5

******