

Time: 3hrs

[Max Marks:80]

- N.B. :** (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1 Attempt any FOUR.

[20]

- a What makes the network vulnerable? List two active and passive attacks.
- b What is Tunneling? How and why is it used in a Virtual Private Network (VPN)?
- c Compare and contrast phishing and pharming.
- d What is PUF? State benefits and drawbacks of PUF.
- e Write a note on a lightweight cryptographic algorithm.
- a Explain the need and outline the functions of an Intrusion Detection System (IDS). [10]
Differentiate between signature-based and anomaly-based IDS.
- b What are various social engineering attacks? Discuss several guidelines to prevent social engineering attacks. [10]
- a What is a confusion matrix? Explain any two biometric authentication schemes in detail. [10]
How do False Negatives adversely affect any biometric authentication Scheme?
- b Outline the top ten security projects in OWASP with their analysis. [10]
- a What are zombies with respect to a DDOS Attack? What are the various types of DOS/DDOS-Attacks? Explain any four in detail. [10]
- b i) Compare and contrast between WEP, WPA and WPA2. [05]
ii) Explain ethical hacking and various phases of ethical hacking. [05]
- a What are the various types of Firewalls? Explain their working in detail. [10]
- b i) How power consumption attacks help an attacker to gather information from the cryptosystem? [05]
ii) What is DVWA? Explain the applications of a framework such as DVWA. [05]
- a How is a Hash obtained from the initial plaintext? Explain any one Hashing algorithm in detail. [10]
- b Write short note on the following (any two) [10]
 - i) SSL
 - ii) Clickjacking and cross site scripting
 - iii) Significance of Honeypots