[Max Marks:80]

Time: 3hrs

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.   [20]

1   **Attempt any FOUR.**

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.   [10]

a   Explain the need and outline the functions of an Intrusion Detection System (IDS).
     Differentiate between signature-based and anomaly-based IDS.   [10]

b   What are various social engineering attacks? Discuss several guidelines to prevent social   [10]
     engineering attacks.

a   What is a confusion matrix? Explain any two biometric authentication schemes in detail.
     How do False Negatives adversely affect any biometric authentication Scheme?   [10]

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.   [05]

b   i) Compare and contrast between WEP, WPA and WPA2.   [05]
     ii) Explain ethical hacking and various phases of ethical hacking.   [10]

a   What are the various types of Firewalls? Explain their working in detail.   [05]

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.   [10]

a   How is a Hash obtained from the initial plaintext? Explain any one Hashing algorithm in   [10]
     detail.

b   Write short note on the following (any two)

     i)   SSL
     ii)   Clickjacking and cross site scripting
     iii) Significance of Honeypots

     _____

40247

F33B634F5009B6E106F98B86CF0E0FB6