R13

Code No: 118GN

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech IV Year II Semester Examinations, May - 2017

INFORMATION SECURITY INCIDENT RESPONSE AND MANAGEMENT

(Common to CSE, IT)

Time: 3 hours **Max. Marks: 75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

(25 Marks)

1.a) Define Bastion Host. [2]
b) What are the advantages of VPN server? [3]
c) What are network devices? [2]
d) Define Modem. [3]
e) Define Information security. [2]
f) What is information security incident and management? [3]
g) What is time synchronization? [2]
h) Define Log. [3]
i) How do we handle malicious code incidents? [2]
j) What is malicious code? [3]

PART - B

(50 Marks)

2.a) Discuss in brief about the steps involved in configuring a Firewall.
b) What are the steps involved in testing the traffic filtering device? [5+5]

OR

3.a) What are the steps involved in configuring a VPN server?
b) Explain in brief about EXEC/ROM user. [5+5]

4.a) What is Trouble shooting? Discuss in brief about methodology of Trouble shooting?
b) Explain in brief about trouble shooting of network devices. [5+5]

OR

5.a) What are the reasons for network slow down?
b) What are the services provided when trouble shooting a network device? [5+5]

6.a) Describe in brief about data back up techniques.
b) Discuss in brief about Incident response roles and responsibilities. [5+5]

OR

7.a) What are the steps involved in developing an effective data back up strategy?
b) Explain in brief about the handling and response of security incident. [5+5]

8.a) Discuss in brief about Log correlation.
b) What are the challenges in Log management? [5+5]

OR

9.a) Explain in brief about Developing Knowledge skills and competences.
b) Describe in brief about Centralized logging and architecture. [5+5]

10.a) What are the steps involved in preparing incident handling?
b) Discuss in brief about Network attacks and security incidents. [5+5]

OR

11.a) Explain in brief about evidence gathering and handling.
b) What are the response strategies in DOS attack? [5+5]