Code No: 128GN **R15**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year II Semester Examinations, July - 2019
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)	What is router?	[2]
b)	Explain about VPN server.	[3]
c)	What is the methodology of troubleshooting?	[2]
d)	Discuss about network slowdowns.	[3]
e)	What is RAID?	[2]
f)	Explain about cloud backup.	[3]
g)	What is Web proxy?	[2]
h)	Explain about SEIM.	[3]
i)	Write the procedure of eradication.	[2]
j)	Describe detection of malicious code.	[3]

PART - B

(50 Marks)

2.	What are configuring modes of network devices? Explain in detail.	[10]
	OR	
3.	Explain in detail about testing the traffic filtering devices.	[10]
4.a)	What are show interfaces commands? Explain.	
b)	Explain about Cisco router basic troubleshooting checklist.	[5+5]
	OR	
5.a)	Write the procedure for minimizing the negative impact of using debug commands.	
b)	Explain about troubleshooting of modems.	[5+5]
6.	Discuss in detail about incident response process.	[10]
	OR	
7.a)	What are incident handling phases? Explain in detail.	
b)	How to pan backup strategy? Explain.	[5+5]

8.a) What are Windows logon types? Explain.
b) Discuss about network quarantine servers. [5+5]

OR

9. Explain in detail about log analysis and storage. [10]

10. Explain the following:
a) Network scanning security incidents
b) Incident handling preparation. [5+5]

OR

11. Explain the following:
a) Evidence gathering and handling
b) Preventing/stopping a DoS incident. [5+5]

---ooOoo---