Bhoj Reddy Engineering College for Women: Hyderabad

Department of Information Technology

Lesson plan of faculty member for the academic year 2017–18

Class: IV B Tech Branch-Section: IT-B Semester: II

Subject: Information Security Incident Response and Management Lectures per week: 4

Lecture Number	Topics to be covered	Date (s)
UNIT-I: Managing Information Security Services		
1	Introduction to Information Security Incident Response & Management	21 December 2017
2	Introduction to Managing Information Security Services	21 December 2017
3	Configuring Network Devices Hub and Switch	22 December 2017
4	Configuring Network Devices Router	23 December 2017
5	Identifying Unauthorized Devices, Identifying Assets	28 December 2017
6	Asset Inventory Tool	28 December 2017
7	Testing the Traffic Filtering Devices	29 December 2017
8	Stateless /Packet Firewall	30 December 2017
9	State full Firewall Technologies	4 January 2018
10	Solutions combining Traffic Filtering with other Technologies	4 January 2018
11	Explaining Snort Tool	5 January 2018
12	Configuring Router, Modes	6 January 2018
13	Configuring Router/Global/Interface/Line/	11 January 2018
14	Configuring Privilege EXEC/ROM/User EXEC	11 January 2018
15	Configuring a Banner/Firewall, Bastion Host/VPN server etc.	12 January 2018
UNIT-II: Troubleshooting Network Devices and Services		
16	Introduction & Methodology of Troubleshooting	13 January 2018
17	Troubleshooting Types	18 January 2018
18	Troubleshooting of Network Communication-Connectivity	18 January 2018
19	Troubleshooting of Network Devices	19 January 2018
20	Troubleshooting of Network Slowdowns-Modems etc.	20 January 2018
UNIT-III: **Information Security Incident Management & Data Backup**		
21	Information Security Incident Management Overview-Handling-Response	25 January 2018
22	Incident Response Roles	25 January 2018
23	Incident Response Responsibilities	27 January 2018
24	Incident Response Process	1 February 2018
25	Data Backup Introduction	1 February 2018
26	Data Backup Techniques	2 February 2018
27	Types of Data Backups	3 February 2018
28	Developing an Effective Data Backup Strategy	10 February 2018
29	Implementing Plan	15 February 2018
30	Types of Security Policies	15 February 2018
31	Security policy for Back Procedures	16 February 2018
UNIT-IV: **Log Correlation**		
32	Computer Security Logs	17 February 2018

Lecture Number	Topics to be covered	Date (s)
33	Configuring Windows Logs	22 February 2018
34	Analyzing Windows Logs	22 February 2018
35	Log Management Functions	23 February 2018
36	Challenges in Log Management	24 February 2018
37	Centralized Logging and Architecture	2 March 2018
38	Time Synchronization Reasons	3 March 2018
39	NTP	8 March 2018
40	NIST	8 March 2018
UNIT-V: **Handling Network Security Incidents & Handling Malicious Code Incidents**		
41	Network Reconnaissance Incidents	9 March 2018
42	Network Scanning Security Incidents	10 March 2018
43	Network Attacks and Security Incidents	15 March 2018
44	Detecting DoS Attack	15 March 2018
45	DoS Response Strategies	16 March 2018
46	Preventing a DoS Incident etc.	17 March 2018
47	Stopping a DoS Incident etc.	22 March 2018
48	Incident Handling Preparation	22 March 2018
49	Detection of Malicious Code	23 March 2018
50	Evidence Gathering	24 March 2018
51	Handling Evidences	29 March 2018
52	Eradication and Recovery.	29 March 2018
53	Revision & Previous year Questions	31 March 2018

Text books:

1. Managing Information Security Risks, The Octave Approach by Christopher Alberts, and Audrey Dorofee.
2. “Cryptography and Network Security (4th Edition) by (Author) William Stallings.”

Name and signature of the faculty: Mr K Sandeep Kumar

Name and signature of Head of the Department: Mr M Vinod