GMR Institute of Technology
An Autonomous Institute Affiliated to JNTUK, Kakinada

GMRIT
Training Tomorrow's Engineers Today

COURSE HANDOUT

B.Tech. - 8th Semester

Course Title : Security Analyst-III **Dated: 27-11-2017**

Course Code : CSE 4436 **Academic Year 2017-18**

Course Structure : 4-1-0-4

Course coordinator : K. Lakshmana rao

Instructor(s) : K. Lakshmana rao

Prerequisite: Web technologies, cryptography & network security, computer networks and security analyst-II.

1. Course Description:

The main intention of this course is to make the students to enrich their skills in Information security management system standard. Configuring network devices gives exposure to concepts like router configuration,router configuration modes. Information security Incident management & Data Backup, Handling Network Security Incidents,Handling Malicious code incidents.

2. Scope and Objective of the Course:

The course content enables students to

- Understand basic security metrics used for individual/organization.
- Recognize basic need of security audit used to find vulnerabilities/threats.
- Understand different vulnerability management process.
- Know how to conduct configuration reviews.

Course Outcomes:
At the end of the course students will be able to:

C_{CS}436.1: Suggest appropriate security management system for individual/organization
C_{CS}436.2: Outline various techniques for configuring network devices.
C_{CS}436.3: Explain various techniques for configuring router.
C_{CS}436.4: Examine different information security Incident management methods.
C_{CS}436.5: Investigate various data backup methods & malicious code anomalies.
C_{CS}436.6: Asses suitable method to handle network security & malicious code incidents.

3. Text Books:

1. NASSCOM Study Material

Reference books:

1. NASSCOM Study Material

4. SYLLABUS:

UNIT I: Managing Information Security Services **(11+4) Hours**

Information security management system standard(ISMS),Configuring Network Devices, Identifying unauthorized Devices, Configuring Router, configuring modes- User EXEC/Privileged EXEC/Global Config/Interface Config/Setup configuring.

UNIT II **(12+4) Hours**

Configuring router banner/Firewall/VPN server. Linux Network Configuration and Troubleshooting-Commands:ifconfig,ifup,ifdown,ping,Traceroute,netstat,dig,nslookup,route,host,arp,ethtool,iwconfig,hostname and system-config-network.

UNIT – III: **(10+3) Hours**

Information security Incident management & Data Backup

Information security Incident management overview-Handling-Response, Incident Response Roles and Responsibilities, incident response process.

Data Backup introduction, Types of data Backup and its techniques, developing an effective data backup strategy and plan, security policy for data backup procedure.

UNIT –IV: **(12 +4) Hours**

Handling Network Security Incidents:

Network Reconnaissance Incidents, Network Scanning Security incidents, Network attacks security incidents, detecting DoS attack, strategies to prevent/stop a DoS incident.

Handling Malicious code incidents:

Incident Handling Preparation, Incident Prevention, Detection of Malicious code, Evidence Gathering and handling, Eradication and recovery, Recommendations.

5. Course Plan:

No. Lecture	Learning objectives	Topic(s) to be covered	Chapter in the textbook/reference
UNIT-I			
1	Information security management system standard(ISMS)	Introduction(ISMS),Process approach and PDCA model	NASSCOM Study Material
2	Information security management system standard(ISMS)	PDCA model,The processes used is PDCA model.	NASSCOM Study Material
3	Information security management system standard(ISMS)	**ISO/IEC27002:2005:**Control objectives and controls	NASSCOM Study Material
4	Configuring Network Devices	The Network Devices and its configuration	NASSCOM Study Material
5	**Tutorial-I**		
6	Identifying unauthorized Devices	Identifying unauthorized Devices	NASSCOM Study Material
7	Configuring Router	configuring modes- User EXEC	NASSCOM Study Material
8	Configuring Router	Privileged EXEC & Global Configuration	NASSCOM Study Material
9	**Tutorial-II**		

10	Configuring Router	Privileged EXEC & Global Configuration	NASSCOM Study Material
11	Configuring Router	Interface and Setup configuring	NASSCOM Study Material
12	**Tutorial-III**		
13	Configuring Router	banner/Firewall	NASSCOM Study Material
14	Configuring Router	banner/Firewall	NASSCOM Study Material
15	**Tutorial-IV**		
UNIT-II			
16	Configuring Router	banner/Firewall	NASSCOM Study Material
17	Configuring Router	VPN server	NASSCOM Study Material
18	**Tutorial-5**		
19	Linux Network Configuration and Troubleshooting-Commands	ifconfig,ifup,ifdown	NASSCOM Study Material
20	Linux Network Configuration and Troubleshooting-Commands	ifconfig,ifup,ifdown	NASSCOM Study Material
21	**Tutorial-6**		
22	Linux Network Configuration and Troubleshooting-Commands	ping, Traceroute	NASSCOM Study Material
23	Linux Network Configuration and Troubleshooting-Commands	netstat,dig	NASSCOM Study Material
24	**Tutorial-7**		
25	Linux Network Configuration and Troubleshooting-Commands	nslookup, route	NASSCOM Study Material
26	Linux Network Configuration and Troubleshooting-Commands	host,arp	NASSCOM Study Material
27	**Tutorial-8**		
28	Linux Network Configuration and Troubleshooting-Commands	ethtool	NASSCOM Study Material
29	Linux Network Configuration and Troubleshooting-Commands	iwconfig	NASSCOM Study Material
30	Linux Network Configuration and Troubleshooting-Commands	hostname and system-config-network.	NASSCOM Study Material
31	Linux Network Configuration	system-config-network.	NASSCOM

	&Troubleshooting-Commands		Study Material
UNIT-III			
32	Information security Incident management	overview-Handling-Response	NASSCOM Study Material
33	Information security Incident management	overview-Handling-Response	NASSCOM Study Material
34	**Tutorial-9**		
35	Information security Incident management	Incident Response Roles and Responsibilities.	NASSCOM Study Material
36	Information security Incident management	incident response process.	NASSCOM Study Material
37	**Tutorial-10**		
38	Data Backup introduction	Data Backup introduction	NASSCOM Study Material
39	Data Backup	Types of data Backup and its techniques	NASSCOM Study Material
40	Data Backup	developing an effective data backup strategy and plan	NASSCOM Study Material
41	Data Backup	developing an effective data backup strategy and plan	NASSCOM Study Material
42	Data Backup	security policy for data backup procedure	NASSCOM Study Material
43	**Tutorial-11**		
44	Data Backup	security policy for data backup procedure	NASSCOM Study Material
UNIT-IV			
45	Handling Network Security Incidents	Network Reconnaissance Incidents.	NASSCOM Study Material
46	Handling Network Security Incidents	Network Scanning Security incidents	NASSCOM Study Material
47	Handling Network Security Incidents	Network Scanning Security incidents	NASSCOM Study Material
48	Handling Network Security Incidents	Network attacks security incidents	NASSCOM Study Material
49	**Tutorial-12**		
50	Handling Network Security	detecting DoS attack	NASSCOM

	Incidents		Study Material
51	Handling Network Security Incidents	strategies to prevent/stop a DoS incident	NASSCOM Study Material
52	Handling Network Security Incidents	strategies to prevent/stop a DoS incident	NASSCOM Study Material
53	**Tutorial-13**		
54	Handling Malicious code incidents	Incident Handling Preparation, Incident Prevention	NASSCOM Study Material
55	Handling Malicious code incidents	Incident Handling Preparation, Incident Prevention	NASSCOM Study Material
56	**Tutorial-14**		
57	Handling Malicious code incidents	Detection of Malicious code	NASSCOM Study Material
58	Handling Malicious code incidents	Evidence Gathering and handling	NASSCOM Study Material
59	**Tutorial-15**		
60	Handling Malicious code incidents	Eradication and recovery, Recommendations	NASSCOM Study Material

6. **Evaluation Procedure**:

Component	Duration (minutes)	Marks	% of weightage	Date & Time	Venue
Sessional Test – 1	90	20	20%	1-01-2018 to 06-01-2018 9:00 AM – 10.30 AM	Block-5
Sessional Test – 2	90	20		15-01-2018 to 10-02-2018 9:00 AM – 10.30 AM	Block-5
Sessional Test – 3	90	20		26-03-2018 to 31-03-2018 9:00 AM – 10.30 AM	Block-5
Comprehensive quiz examination	20	10	10%	26-03-2018 to 31-03-2018	CA Lab.
External Examination	**180**	**70**	**70%**	09-04-2018 to 21-04-2018	Block-5

7. **Chamber Consultation Hour**: 4 to 5PM
Venue: Class Room in Block-5

Notices: Block-5 Notice board

Signature of the Instructors
(K.Lakshmana rao)

Signature of the course-coordinator
(K.Lakshmana rao)