


J.B. INSTITUTE OF ENGINEERING & TECHNOLOGY

(AUTONOMOUS)



ACADEMIC YEAR

2013-14


	COURSE PLAN	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: K.ROSHAN & M.A.MUNEER
 Designation: Assoc.Professor Asst. Professor
 Department:: Information Technology

COURSE DETAILS

Name Of The Programme:: B.TECH Batch:: 2011
 Designation :: Assistant Professor
 Year III Semester 2 nd
 Department:: Information Technology
 Title of The Subject Network Security Subject Code 6756030
 No of Students 84

	COURSE PLAN	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
 Designation: Assistant Professor
 Department:: Information Technology

1. TARGET

- a) Percentage Pass :- 100
- b) Percentage I class 80

2. COURSE PLAN

- 1. Teaching the students in the class
- 2. Mentioning the Engineering applications.
- 3. Text book exercises.
- 4. Assignments.

3. METHOD OF EVALUATION

- 3.1. Continuous Assessment Examinations (CAE 1, CAE 2) : YES/~~NO~~
- 3.2. Assignments / Seminars : YES/~~NO~~
- 3.3. Mini Projects : YES/~~NO~~
- 3.4. Quiz : YES/~~NO~~
- 3.5. Term End Examination : YES/~~NO~~
- 3.6. Others : YES/~~NO~~

Signature of HOD
Date:

Signature of Faculty
Date:



GUIDELINES TO STUDY THE SUBJECT

2013-14

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

Guidelines for Preparing the Course:

Course Description:

This course is to provide students with an overview of the concepts and fundamentals of data To provide a practical survey of Network Security Applications and standards. The Emphasis is on applications that are widely used on the Internet and for corporate networks and on standards, especially Internet standards that have been widely deployed, and discuss common security weaknesses, vulnerabilities, attack methods, and mitigation approaches. This course will provide a comprehensive list of security issues related to general networking design and development.

Course Objectives:

At the end of the course, the students will be able to:

1. Understand security concepts, Ethics in Network Security.
2. Understand security threats, and the security services and mechanisms to counter them
3. Comprehend and apply relevant cryptographic techniques
4. Comprehend security services and mechanisms in the network protocol stack
5. Comprehend and apply authentication services and mechanisms
6. Comprehend and apply relevant protocol like SSL, SSH etc.
7. Comprehend and apply email security services and mechanisms
8. Comprehend and apply web security services and mechanisms
9. Comprehend computer and network access control

Learning Outcomes:

1. Should be able to identify network security threats and determine efforts to counter them
2. Should be able to write code for relevant cryptographic algorithms.
3. Should be able to write a secure access client for access to a server



COURSE OBJECTIVES

2013-14

Regulation: R11

4. Should be able to send and receive secure mail
5. Should be able to determine firewall requirements, and configure a firewall

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology

On completion of this Subject / Course the student shall be able to:

S.No	Objectives	Outcomes
1.	Understand security concepts, Ethics in Network Security.	A,B,C,D,E
2.	Understand security threats, and the security services and mechanisms to counter them	C,D,E,F
3	Comprehend and apply relevant cryptographic techniques	A,D,C,E
4	Comprehend security services and mechanisms in the network protocol stack	A,B,C,D,E,F
5	Comprehend and apply authentication services and mechanisms	A,D,C,E
6	Comprehend and apply relevant protocol like SSL, SSH etc.	C,B,D,F,H,I,J
7	Comprehend and apply email security services and mechanisms	C,D,H,I,J,K
8	Comprehend and apply web security services and mechanisms	A,B,F,E,G,H,I

Signature of Faculty
Date:

Note: For each of the OBJECTIVE indicate the appropriate OUTCOMES to be achieved.
Kindly refer Page 16, to know the illustrative verbs that can be used to state the objectives.



COURSE OUTCOMES

2013-14

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
 Designation: Assistant Professor
 Department:: Information Technology

The expected outcomes of the Course / Subject are:

S.No	General Categories of Outcomes	Specific Outcomes of the Course
A.	An ability to apply knowledge of mathematics, science, and engineering	1,2 ,3 6,7
B.	An ability to design and conduct experiments, as well as to analyze and interpret data	1,3,4,6,7
C.	An ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability and sustainability	2,4,6,8,9
D.	An ability to function on multi-disciplinary teams	1,3,4,5,6,7
E.	An ability to identify, formulate, and solve engineering problems	1,2,3,5,6,8,9
F.	An understanding of professional and ethical responsibility	1,2,3,4,5,6
G.	An ability to communicate effectively	3,4,5,6,8
H.	The broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context	2,3,4,5,6
I.	A recognition of the need for, and an ability to engage in life-long learning	1,2,3,4,8,9
J.	A knowledge of contemporary issues	2,3,6,8,9,10
K.	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.	3,5,6,8,9,10

Objectives – Outcome Relationship Matrix (Indicate the relationships by ☒ mark).

Objectives \ Outcomes	A	B	C	D	E	F	G	H	I	J	K
1.	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒
2.	☒	☐	☒	☒	☐	☒	☐	☒	☒	☒	☒
3.	☐	☒	☐	☒	☒	☐	☒	☒	☐	☐	☒
4.	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☒
5.	☒	☒	☐	☒	☒	☐	☐	☐	☒	☐	☒
6.	☒	☒	☒	☐	☐	☒	☒	☒	☒	☒	☐
7.	☒	☐	☒	☒	☒	☐	☐	☐	☐	☐	☒
8.	☒	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒
9.	☒	☐	☒	☒	☒	☐	☒	☐	☒	☐	☒
10.	☐	☒	☐	☐	☒	☒	☒	☒	☒	☒	☒



COURSE SCHEDULE

2013-14

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
 Designation: Assistant Professor
 Department:: Information Technology

The Schedule for the whole Course /
 Subject is::

S. No	Description	Duration (Date)		Total No. of Periods
		From	To	
1.	Security attacks,(Interruption, Interception, Modification and Fabrication) Security Services (Confidentiality, Authentication ,Integrity, Non-repudiation, access control and Availability), and Mechanisms, A Model for Internetwork Security, Internet Standards and RFCs. Buffer overflow & format string vulnerabilities. TCP session hijacking, ARP attacks route table modifications. UDP hijacking, and man-in-the-middle attacks	20-12-2013	03-01-2014	10
2.	Conventional Encryption Principles, algorithms Cyper block modes of operation, location of encryption devices key distribution approaches of Message Authentication. Secure hash functions and HMAC	04-01-2014	21-01-2014	8
3.	Public key cryptography principles Public key cryptography algorithms , digital signatures, Digital certificates, Certificate authority and key management Kerberos , X.509 Directory authentication service.	22-01-2014	31-01-2014	8
4.	Email privacy, pretty good privacy(PGP) and S/MIME	03-02-2014	17-02-2014	8
5.	IP Security Overview , IP Security architecture , Authentication Header Encapsulating Security payload, combining security associations and Key Management	18-02-2014	28-02-2014	8
6.	Web security requirements, Secure Socket Layer (SSL) and Transport Layer Security(TLS), Secure Electronic Transaction	01-03-2014	11-03-2014	8

	(SET)			
7	Basic concepts of SNMP, SNMPv1, Community facility and SNMPv3 ,Intruders, Viruses and related threats			8
8	Firewall design principles, Trusted Systems, Intrusion Detection Systems.			7

Total No. of Instructional periods available for the course: **65**

Hours / Periods 50 Minutes

Books / Material

Text Books (TB)

TB1: Network Security Essentials (Applications and Standards)

By William Stallings Pearson Education.

TB2: Hack Proofing your network by Ryan Russell. Dan Kaminsky,

Rain forest Puppy, Joe Grand , David Ahmed , Hal Flynn etc.

Suggested / Reference Books (RB)

RB1: Network security and cryptography : Bernard Menzes, CENGAGE Learning

**RB2: Network Security-private communication in a public world by Charlie Kaufman
Radia Perlman and Mike Speciner Pearson /PHI**

RB3: Cryptography Network Security . III edition Stallings . PHI/ Pearson

RB4: Principles of information Security, Whiteman Cengage Learning

**RB5: Cryptography and Network Security : B.A.Forouzen D Mukhophadhayaya Second
edition , TMH**



SCHEDULE OF INSTRUCTIONS

2013-14

UNIT - I

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole

Course / Subject is::65

Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome Nos.	References (Text Book, Journal...) Page No ___ to ___
1	20-12-2013	1	Security attacks,(Interruption, Interception, Modification and Fabrication	1,2,4	T1:7-11
2	21-12-2013	1	Security Services (Confidentiality, Authentication ,Integrity, Non-repudiation, access control and Availability), and	1,4,5	T1:11-14
3	23-12-2013	1	Mechanisms, A Model for Internetwork Security,	1.2.6	T1:14-9
4	24-12-2013	1	Internet Standards and RFCs	1,3,4	T1:19-22
5	27-12-2013 28-12-2013	2	Buffer overflow & format string vulnerabilities	1	T1:
6	30-12-2013 31-12-2013	2	Secure hash functions and HMAC TCP session hijacking,	1	T1:
7	01-01-2014 03-01-2014	2	ARP attacks route table modifications. UDP hijacking, and man-in-the-middle attacks	1	T1:


Signature of Faculty

Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

3. MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - II	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::


Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1	04-01-2014	1	Conventional Encryption Principles,	2	T1:29-35
2	06-01-2014	1	Conventional Encryption algorithms,	2	T1:35-45
3	08-01-2014	1	Cipher block modes of operation,	2	T1:46-50
4	10-01-2014	1	location of encryption devices	2	T1:51-52
5	10-01-2014	1	key Distribution,	2	T1:53-55
6	20-01-2014	1	approaches of Message Authentication.	2	T1:60-64
7	20-01-2014	1	Secure hash functions	2	T1:64-72
8	21-01-2014	1	HMAC	2	T1:72-73

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - III	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::


Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1	22-01-2014	1	Public key cryptography principles	3	T1:74-77
2	22-01-2014 24-01-2014	2	Public key cryptography algorithms	3	T1:78-84
3	25-01-2014	1	digital signatures	3	T1:85
4	27-01-2014	1	Digital certificates	3	T1:86-87
5	28-01-2014 29-01-2014	2	Certificate authority and key management Kerberos ,	3	T1:95-112
6	31-01-2014	1	X.509 Directory authentication service.	3	T1:113-122

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - IV	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::

Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1	03-02-2014 04-02-2014	2	Email privacy,	4	T1:132-135
2	05-02-2014 07-02-2014 10-02-2014	3	pretty good privacy(PGP)	4	T1: 136-150
3	11-02-2014 12-02-2014 17-02-2014	3	S/MIME	4	T1:151-168


Signature of Faculty

Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - V	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::


Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1	18-02-2014	1	IP Security Overview	5	T1:179-181
2	19-02-2014 21-02-2014	2	IP Security architecture	5	T1:182-187
3	22-02-2014 24-02-2014	2	Authentication Header		T1:187-192
4	25-02-2014	1	Encapsulating Security payload,	5	T1:192-196
5	26-02-2014	1	combining security associations		T1:197-200
6	28-02-2014	1	Key Management	5	T1:200-210

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - VI	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::


Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1	01-03-2014 03-03-2014	2	Web security requirements	6	T1:222-225
2	04-03-2014 05-03-2014	2	Secure Socket Layer (SSL)	6	T1:225-238
3	07-03-2014 08-03-2014	2	Transport Layer Security(TLS)	6	T1:238-243
4	10-03-2014 11-03-2014	2	Secure Electronic Transaction (SET)	6	T1:243-254

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - VII	2013-14
		Regulation: R11


FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
 Designation: Assistant Professor
 Department:: Information Technology
 The Schedule for the whole Course / 65
 Subject is::

Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1		1	Basic concepts of SNMP	7	T1:258-266
2		2	SNMPv1 Community facility	7	T1:266-268
3		2	SNMPv3	7	T1:269-292
4		2	Intruders	7	T1:299-302
5		1	Viruses and related threats	7	T1:330-340

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.
 2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.
 MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	SCHEDULE OF INSTRUCTIONS UNIT - VIII	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology

The Schedule for the whole Course / 65

Subject is::

Sl. No.	Date	No. of Periods	Topics / Sub - Topics	Objectives & Outcome	References (Text Book, Journal...)
				Nos.	Page No to
1		2	Firewall design principles,	8	T1:353-365
		3	Trusted Systems		T1:365-370
2		2	Intrusion detection systems	8	T1:302-313

Signature of Faculty
Date

Note: 1. ENSURE THAT ALL TOPICS SPECIFIED IN THE COURSE ARE MENTIONED.

2. ADDITIONAL TOPICS COVERED, IF ANY, MAY ALSO BE SPECIFIED **BOLDLY**.

MENTION THE CORRESPONDING COURSE OBJECTIVE AND OUT COME NUMBERS AGAINST EACH TOPIC.

	COURSE COMPLETION STATUS	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Subject:: Computer Networks

Subject

Code:

6756030

Department::Information

Technology

Actual Date of Completion & Remarks, if any

Units	Remarks	Nos. of Objectives Achieved
Unit 1	Topics are Completed	1,2,4,6,8
Unit 2	Topics are Completed	1,2,4,6,8
Unit 3	Topics are Completed	2,3,6,8
Unit 4	Topics are Completed	1,2,3,5,6
Unit 5	Topics are Completed	1,2,3,5,6
Unit 6	Topics are Completed	1,2,4,6,8,10
Unit 7	Topics are Completed	1,3,4,5,6,7
Unit 8	Topics are Completed	1,2,3,4,6,10

Signature of Dean of School

Date:

Signature of Faculty

Date:

NOTE: AFTER THE COMPLETION OF EACH UNIT MENTION THE NUMBER OF OBJECTIVES ACHIEVED.



TUTORIAL SHEETS - I

2013-14

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology
The Schedule for the whole Course / 65
Subject is::

Date:

This Tutorial corresponds to Unit Nos. I

Time:

DESCRIPTIVE QUESTIONS:

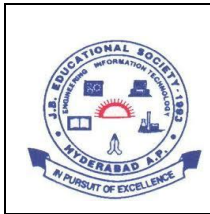
1. What is the difference between passive and active security threats?
2. List few examples of software attacks?
3. List and briefly define program (software) threats?
4. What is the OSI security architecture?

5. List and briefly define categories of passive and active security attacks?
6. Explain the network security model)

Please write the Questions / Problems / Exercises which you would like to give to the students and also mention the objectives to which these questions / Problems are related.

Signature of Dean of School
Date:

Signature of Faculty
Date:



TUTORIAL SHEETS - II

2013-14

Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology
The Schedule for the whole Course / 65
Subject is::

Date:

This Tutorial corresponds to Unit Nos. II

Time:


DESCRIPTIVE QUESTIONS:

1. What are the two basic functions used in encryption algorithms?
2. What are the essentials ingredients of a symmetric cipher?
3. Compare DES, 3DES, and AES?
4. What is the difference between a session key and a master key?
5. What is the difference between a block cipher and a stream cipher ?
6. What is the difference between a link and end to end encryption?
7. What are the advantages of key distributions?

Please write the Questions / Problems / Exercises which you would like to give to the students and also mention the objectives to which these questions / Problems are related.

Signature of Dean of School
Date:

Signature of Faculty
Date:

	TUTORIAL SHEETS - III	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology

Date:

This Tutorial corresponds to Unit Nos.III

Time:

DESCRIPTIVE QUESTIONS:

1. List three approaches to message authentication?
2. What is a message authentication code?
3. List HMCA Design objectives?
4. How is MA Different from HMAC?
5. What is the difference between a private key and a secret key?
6. What is the digital signature?
7. What is a public key certificate?
8. Explain different crypto algorithms where public key crypto systems are used?


Please write the Questions / Problems / Exercises which you would like to give to the students and also mention the objectives to which these questions / Problems are related.

Signature of Dean of School

Date:

Signature of Faculty

Date:

	TUTORIAL SHEETS - IV	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology


Date:

This Tutorial corresponds to Unit Nos. **IV**

Time:

DESCRIPTIVE QUESTIONS:

1. What are the five principal services provided by PGP.
2. Why does PGP generates a signature before applying compression.
- 3why is segmentation and reassembly function in PGP needed.
4. What are different cryptographic algorithms used in S/MIME.
- 5.Explain how S/MIME is better than MIME.

	TUTORIAL SHEETS - V	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology


Date:

This Tutorial corresponds to Unit Nos. **V**

Time:

DESCRIPTIVE QUESTIONS:

1. Explain about the IP security overview and its architecture.
2. Discuss in detail about the encapsulating security payload
3. What is the role of key management in IPSec. Explain
4. Explain about the combining security associations.

	TUTORIAL SHEETS – VI	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
Designation: Assistant Professor
Department:: Information Technology


Date:

This Tutorial corresponds to Unit Nos: **VI**

Time:

DESCRIPTIVE QUESTIONS:

- 1.what services are provided by the SSL Record protocol.
- 2.Expalin about the Web security requirements.
- 3.Differentiate between secure socket layer and transport layer security.
- 4.what is SET.Explain secure electronic commerce components

	TUTORIAL SHEETS - VII	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER

Designation: Assistant Professor

Department:: Information Technology


date:

Time:

This Tutorial corresponds to Unit Nos: **VII**

DESCRIPTIVE QUESTIONS:

1. What are the basic concepts of SNMP? Explain.
2. How SNMP is different from SNMP1.
3. Write short notes on intruders.
4. Explain about the viruses and their related threats

	TUTORIAL SHEETS - VIII	2013-14
		Regulation: R11

FACULTY DETAILS:

Name of the Faculty:: M.A.MUNEER
 Designation: Assistant Professor
 Department:: Information Technology

t
date:

This Tutorial corresponds to Unit Nos.VIII

Time:

DESCRIPTIVE QUESTIONS:

1. What are the firewall design principles and characteristics explain.
2. Explain about the concept of trusted systems.
3. Discuss in detail about the intrusion detection systems.

	ILLUSTRATIVE VERBS FOR STATING INSTRUCTIONAL OBJECTIVES	2013-14
		Regulation: R11

These verbs can also be used while framing questions for Continuous Assessment Examinations as well as for End – Semester (final) Examinations.

ILLUSTRATIVE VERBS FOR STATING GENERAL OBJECTIVES

Know Comprehend	Understand Apply	Analyze Design	Generate Evaluate
--------------------	---------------------	-------------------	----------------------

ILLUSTRATIVE VERBS FOR STATING SPECIFIC OBJECTIVES:

A. Cognitive Domain

1	2	3	4	5	6
Knowledge	Comprehension Understanding	Application of knowledge & comprehension	Analysis of whole w.r.t. its constituents	Synthesis combination of ideas/constituents	Evaluation judgement

Define	Convert	Change	Breakdown	Categorize	Appraise
Identify	Defend	Compute	Differentiate	Combine	Compare
Label	Describe (a	Demonstrate	Discriminate	Compile	Conclude
List	procedure)	Deduce	Distinguish	Compose	Contrast
Match	Distinguish	Manipulate	Separate	Create	Criticize
Reproduce	Estimate	Modify	Subdivide	Devise	Justify
Select	Explain why/how	Predict		Design	Interpret
State	Extend	Prepare		Generate	Support
	Generalize	Relate		Organize	
	Give examples	Show		Plan	
	Illustrate	Solve		Rearrange	
	Infer			Reconstruct	
	Summarize			Reorganize	
				Revise	

B. Affective Domain		C. Psychomotor Domain (skill development)				
Adhere	Resolve	Bend	Dissect	Insert	Perform	Straighten
Assist	Select	Calibrate	Draw	Keep	Prepare	Strengthen
Attend	Serve	Compress	Extend	Elongate	Remove	Time
Change	Share	Conduct	Feed	Limit	Replace	Transfer
Develop		Connect	File	Manipulate	Report	Type
Help		Convert	Grow	Move precisely	Reset	Weigh
Influence		Decrease	Handle	Operate	Run	
Initiate		Demonstrate	Increase	Paint	Set	



LESSON PLAN
Unit-1

2013-14

Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Computer Networks

Subject 6756030

Code


Unit 1

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
1	Security attacks,(Interruption, Interception, Modification and Fabrication	00:50	T1	Black Board
2	Security Services (Confidentiality, Authentication ,Integrity, Non-repudiation, access control and Availability),	00:50	T1	Black Board
3	Mechanisms, A Model for Internetwork Security,	00:50	T1	Black Board
4	Internet Standards and RFCs	00:50	T1	Black Board
5 & 6	Buffer overflow & format string vulnerabilities	01:40	T1	Black Board
7 & 8	Secure hash functions and HMAC TCP session hijacking,	01:40	T1	Black Board
9 & 10	ARP attacks route table modifications. UDP hijacking, and man-in-the-middle attacks	01:40	T1	Black Board

On completion of this lesson the student shall be able to(Outcomes)

1. Understand the concepts of security attacks, services, mechanisms.
2. able to draw the model of internetwork security
3. The types of ARP attacks and router table modifications


	ASSIGNMENT Unit-I	2013-14
		Regulation: R11

Assignment / Questions

1. 1. What is the difference between passive and active security threats?
2. List few examples of software attacks?
3. List and briefly define program (software) threats?
4. What is the OSI security architecture?
5. List and briefly define categories of passive and active security attacks?
6. Explain the network security model

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-II	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code

Unit II

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
11	Conventional Encryption Principles,	00:50	T1	Black Board
12	Conventional Encryption algorithms,	00:50	T1	Black Board
13	Cipher block modes of operation,	00:50	T1	Black Board
14	location of encryption devices	00:50	T1	Black Board
14	key Distribution,	00:50	T1	Black Board
16	approaches of Message Authentication.	00:50	T1	Black Board
17	Secure hash functions	00:50	T1	Black Board
18	HMAC	00:50	T1	Black Board

On completion of this lesson the student shall be able to

1. Know about Conventional Encryption Principles and algorithms.
- 2 the types of Cipher block modes of operation,
3. The working of the key Distribution
4. The different approaches of message authentication



**ASSIGNMENT
Unit-II**

2013-14

Regulation: R11

Assignment / Questions

1. What are the two basic functions used in encryption algorithms?
2. What are the essential ingredients of a symmetric cipher?
3. Compare DES, 3DES, and AES?
4. What is the difference between a session key and a master key?
5. What is the difference between a block cipher and a stream cipher?
6. What is the difference between a link and end to end encryption?
7. What are the advantages of key distributions?

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.



LESSON PLAN
Unit-III

2013-14

Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code


Unit III

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
19	Public key cryptography principles	00:50	T1	Black Board
20 & 21	Public key cryptography algorithms	01:40	T1	Black Board
22	digital signatures	00:50	T1	Black Board
23	Digital certificates	01:40	T1	Black Board
24 & 25	Certificate authority and key management Kerberos ,	01:40	T1	Black Board
26	X.509 Directory authentication service.	00:50	T1	Black Board

On completion of this lesson the student shall be able to(Outcomes)

1. about the Public key cryptography principles and algorithms
2. Digital signatures and digital certificates
3. Certificate authority and key management.
4. the application of Kerberos and its services

	ASSIGNMENT Unit-III	2013-14
		Regulation: R11

Assignment / Questions

1. 1. List three approaches to message authentication?
2. What is a message authentication code?
3. List HMCA Design objectives?
4. How is MA Different from HMAC?
5. What is the difference between a private key and a secret key?
6. What is the digital signature?
7. What is a public key certificate?
8. Explain different crypto algorithms where public key crypto systems are used?

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-IV	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code


Unit IV

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
27 & 28	Email privacy,	01:40	T1	Black Board
29,30 & 31	pretty good privacy(PGP)	02:30	T1	Black Board
32,33 & 34	S/MIME	02:30	T1	Black Board

On completion of this lesson the student shall be able to (Outcomes)

1. What is PGP and the working of PGP.
2. The applications of PGP.
3. The architecture of S/SMIME


	ASSIGNMENT Unit-IV	2013-14
		Regulation: R11

Assignment / Questions

1. What are the five principles services provided by PGP.
2. What is the utility of a detached signature?
3. Why is R64 conversion useful for an e-mail application.
4. List the different MIME content types

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-V	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code


Unit V

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
35	IP Security Overview	00:50	T1	Black Board
36 & 37	IP Security architecture	01:40	T1	Black Board
38 & 39	Authentication Header	01:40		
40	Encapsulating Security payload,	00:50		
41	combining security associations	00:50		
42	Key Management	00:50	T1	Black Board

On completion of this lesson the student shall be able to (Outcomes)

1. To give an example of application of IP security.
2. What services are provided by IP security.
3. What parameters identify an SA and what parameters characterize the nature of a particular SA.
4. Why does ESP include a padding field.


	ASSIGNMENT Unit-V	2013-14
		Regulation: R11

Assignment / Questions

1. Discuss in detail about the IP security overview and its architecture.
2. What is the use of the authentication header? How does it works
3. The ESP format and tunnel modes and transport mode.
4. What are the services and applications of key management

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-VI	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code


Unit VI

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
43 & 44	Web security requirements	01:40	T1	Black Board
45 & 46	Secure Socket Layer (SSL)	01:40	T1	Black Board
47 & 48	Transport Layer Security(TLS)	01:40	T1	Black Board
49 & 50	Secure Electronic Transaction (SET)	01:40	T1	Black Board

On completion of this lesson the student shall be able to (Outcomes)

1. The considerations of web security.
2. SSL architecture, Record Protocol and SSIL stack.
3. SSL Record protocol operation.
4. TLS alert codes and types of client certificate .


	ASSIGNMENT Unit-VI	2013-14
		Regulation: R11

Assignment / Questions

1. what are the advantages of each of the three approaches TCP/IP protocol stack.
2. List the different alert codes of TLS protocol.
3. What services are provided by the SSL record protocol.
4. What are the advantages of SET protocol.
5. List the handshake protocol message types.

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-VII	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code


Unit VII

**INSTRUCTIONAL
OBJECTIVES:**

Session No	Topics to be covered	Time	Ref	Teaching Method
51	Basic concepts of SNMP	00:50	T1	Black Board
52 & 53	SNMPv1 Community facility	00:50	T1	Black Board
54 & 55	SNMPv3	01:40	T1	Black Board
56 & 57	Intruders	01:40	T1	Black Board
58	Viruses and related threats	00:50	T1	Black Board

On completion of this lesson the student shall be able to

1. The network management architecture.
2. The communities and community names.
3. The SNMP architecture
4. Message processing and the user security model.
5. The View based access control


	ASSIGNMENT Unit-VII	2013-14
		Regulation: R11

Assignment / Questions

1. In what sense is a network management architecture considered integrated.
2. What are the key elements of the SNMP model.
3. What is auto discovery in SNMP protocol. What is the function of an SNMP proxy.
4. What is the role of sub agent in SNMP architecture.
5. Why does SNMP use an unreliable UDP datagrams. What would be the reason for the designers to choose UDP instead of TCP for the transport protocol for SNMP

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.

	LESSON PLAN Unit-VIII	2013-14
		Regulation: R11

Name of the Faculty: M.A.MUNEER

Subject Network Security

Subject 6756030

Code

Unit: VIII


INSTRUCTIONAL
OBJECTIVES:

Session No	Topics to be covered	Time	Ref	Teaching Method
59 & 60	Firewall design principles,	50:00	T1	Black Board
61,62 & 63	Trusted Systems	50:00	T1	Black Board
64 & 65	Intrusion detection systems	50:00	T1	Black Board

On completion of this lesson the student shall be able to

1. The firewall characteristics .The types of Firewalls and configurations.
2. Know about the data access control.
3. The concept of trusted systems.
4. The common criteria for information technology security evaluation.
5. The applications of intrusion detection systems.

6.

	ASSIGNMENT Unit-VIII	2013-14
		Regulation: R11

Assignment / Questions

1. List the three design goals for a firewall.
2. What is IP address spoofing and how can it be prevented using firewalls.
3. What are some weaknesses of a packet-filtering router.
4. What is an application level gateway?
5. What properties are required for a reference monitor?
6. How is a firewall different from intrusion detection systems?

Signature of Faculty

Note: Mention for each question the relevant objectives and outcomes.