Government of Karnataka
Department of Technical Education
Bengaluru

	Course Title: **Network Security Lab**		
	Scheme (L:T:P) : **0:2:4**	Total Contact Hours: **78**	Course Code: **15CS65P**
	Type of Course: **Tutorial and Practical's**	Credit :03	Core/ Elective: **Core**
CIE- 25 Marks			SEE- 50 Marks

Prerequisites

Knowledge of Computer Network Softwares and Components.

Course Objectives

1. Installation of relevant softwares to Demonstrate Virtual box, port scanning, Finding active machines and version of remote OS.
2. Demonstrate active and passive fingerprinting, sniffing the router traffic, use of dumpsec.
3. Perform wireless audit of an access point, ARP poisioning, IPCop installation, study of various crypto algorithms.
4. Demonstrate IDS, Rootkits, Open ssl command, setup and monitoring honeypot.

Course Outcome

On successful completion of the course, the students will be able to attain CO:

Course Outcome		Experiment linked	CL	Linked PO	Teaching Hrs
CO1	Install and demonstrate virtual box or any other equivalent software and Grabbing banner with telnet and netcat	*1, 2*	*A*	1 to 10	**09**
CO2	Demonstrate port scanning, active machines, version of remote OS using NMAP or any other software.	*3,4*	*A*	1 to 10	**12**
CO3	Experiment on active and passive fingerprinting, sniffing the router traffic, use of dumpsec	*5 to 7*	*A*	1 to 10	**15**
CO4	Demonstrate wireless audit of an access point, ARP poisoning, IPCop Firewall installation using relevant softwares.	*8 to 10*	*A*	1 to 10	**18**
CO5	Demostrate different cryptoalgorithms, IDS, Rootkits using suitable softwares.	*11 to 13*		1 to 10	**15**
CO6	Demonstrate open ssl command, setup and monitor honeypot on network.	*14,15*	*A*	1 to 10	**09**
			Total sessions		**78**

Legends: R = Remember U= Understand; A= Apply and above levels (Bloom's revised taxonomy)

Course-PO Attainment Matrix

Course	Programme Outcomes									
	1	2	3	4	5	6	7	8	9	10
Network Security Lab	3	3	3	3	3	3	3	3	3	3

Level 3- Highly Addressed, Level 2-Moderately Addressed, Level 1-Low Addressed.

Method is to relate the level of PO with the number of hours devoted to the COs which address the given PO.
If ≥40% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 3
If 25 to 40% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 2
If 5 to 25% of classroom sessions addressing a particular PO, it is considered that PO is addressed at Level 1
If < 5% of classroom sessions addressing a particular PO, it is considered that PO is considered not-addressed.

List of Graded Practical Exercises

Sl.No	Practical/Exercise
1	Learn to install Wine/Virtual Box/ or any other equivalent s/w on the host OS
2	Perform an experiment to grab a banner with telnet and perform the task using Netcat
3	Perform an experiment for Port Scanning with nmap, superscan or any other equivalent software
4	Using nmap 1)Find Open ports on a system 2) Find machines which are active 3)Find the version of remote OS on other systems 4)Find the version of s/w installed on other system (using nmap or any othe software)
5	Perform an experiment on Active and Passive finger printing using XProbe2 and nmap
6	Perform an experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / wireshark / tcpdump
7	Perform an experiment how to use DumpSec.
8	Perform an wireless audit of an access point / router and decrypt WEP and WPA (softwares netstumbler or airsniff)
9	Perform an experiment to sniff traffic using ARP poisoning
10	Install IPCop on a linux system and learn all the function available on the software.
11	Install JCrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management
12	Demonstrate Intrusion Detection System (IDS) using any tool eg. Snort or any other s/w
13	Install RootKits and study variety of opt
14	Generate minimum 10 passwords of length 12 characters using open ssl command
15	Setup a honey pot and monitor the honey pot on network

Reference

Build Your Own Security Lab: A field guide for network Testing, Michael Gregg, Wiley India edition, ISBN: 9788126516919.

Suggested list of student activities

Note: the following activities or similar activities for assessing CIE (IA) for 5 marks (Any one)

1. Each individual student should do any one of the following type activity or any other similar activity related to the course and before conduction, get it approved from concerned course co-ordinator and programme co-ordinator.
2. Each student should conduct different activity and no repeating should occur.

1.	Demonstration of various software's used for port scanning.
2.	Report on result of various crypto algorithms by using equivalent software.
3.	Prepare a report on firewall along with its uses and functions.

Course Delivery

The course will be delivered through Demonstration and Practices

Course Assessment and Evaluation Scheme

Method	What		To whom	When/Where (Frequency in the course)	Max Marks	Evidence collected	Course outcomes
Direct Assessment	CIE (Continuous Internal Evaluation)	IA	Students	Two tests (average of two tests)	10	Blue books	1,2,3,4,5,6
				Record	10	Record	1,2,3,4,5,6
				Student activity.	05	Report.	
				Total	**25**		
	SEE (Semester End Examination)	End Exam		**End of the course**	**50**	Answer scripts at BTE	1,2,3,4,5,6
Indirect Assessment	Student Feedback on course		Students	Middle of the course		Feedback forms	1,2,3 Delivery of course
	End of Course Survey			End of the course		Questionnaires	1,2,3,4,5,6 Effectiveness of Delivery of instructions & Assessment Methods

*CIE – Continuous Internal Evaluation *SEE – Semester End Examination

Note:

1. I.A. test shall be conducted as per SEE scheme of valuation. However obtained marks shall be reduced to 10 marks. Average marks of two tests shall be rounded off to the next higher digit.
2. Rubrics to be devised appropriately by the concerned faculty to assess Student activities.

Questions for CIE and SEE will be designed to evaluate the various educational components (Bloom's taxonomy) such as:

Sl. No	Bloom's Category	%
1	Remembrance	10
2	Understanding	20
3	Application	70

Note to IA verifier: The following documents to be verified by CIE verifier at the end of semester

1. Blue books (10 marks)
2. Record (10 marks)
3. Student suggested activities report for 5 marks
4. Student feedback on course regarding Effectiveness of Delivery of instructions & Assessment Methods.

Format for Student Activity Assessment

DIMENSION	Unsatisfactory 1	Developing 2	Satisfactory 3	Good 4	Exemplary 5	Score
Collection of data	Does not collect any information relating to the topic	Collects very limited information; some relate to the topic	Collects some basic information; refer to the topic	Collects relevant information; concerned to the topic	Collects a great deal of information; all refer to the topic	3
Fulfill team's roles & duties	Does not perform any duties assigned to the team role	Performs very little duties	Performs nearly all duties	Performs all duties	Performs all duties of assigned team roles with presentation	4
Shares work equally	Always relies on others to do the work	Rarely does the assigned work; often needs reminding	Usually does the assigned work; rarely needs reminding	Does the assigned job without having to be reminded.	Always does the assigned work without having to be reminded and on given time frame	3
Listen to other Team mates	Is always talking; never allows anyone else to speak	Usually does most of the talking; rarely allows others to speak	Listens, but sometimes talk too much	Listens and contributes to the relevant topic	Listens and contributes precisely to the relevant topic and exhibit leadership qualities	3
					TOTAL	13/4=3.25=4

Note: This is only an example. Appropriate rubrics/criteria may be devised by the

concerned Course Coordinator for assessing the given activity

Scheme of Valuation for End Examination

SN	Particulars	Marks
1	Record	05
2	Installation of tool (Any two)	15
3	Conduction and Demonstration	20
4	Viva Voce	10
	Total	**50**

***Evaluation should be based on the screen output only. No hard copy required.*
***Change of question is allowed only once. Marks of 05 should be deducted in the given question.*

Resource requirements for Network Security Lab

(For an Intake of 60 Students [3 Batches])

1) For all experiments the student must and should install software's. After the demonstrate the same be uninstalled. Each batch has to learn to install and use the tools. You can use any other equivalent software's other then the mentioned one.

2) The lab should have structured network with 10 mbps internet line. Using Virutal Box, two OS can be installed on one machine, where in one OS acts as a client and other acts a server.

MODEL QUESTION BANK

1	Learn to install Wine/Virtual Box/ or any other equivalent s/w on the host OS
2	Perform an experiment to grab a banner with telnet and perform the task using Netcat
3	Perform an experiment for Port Scanning with nmap, superscan or any other equivalent software
4	Using nmap 1)Find Open ports on a system 2) Find machines which are active 3)Find the version of remote OS on other systems 4)Find the version of s/w installed on other system (using nmap or any othe software)
5	Perform an experiment on Active and Passive finger printing using XProbe2 and nmap
6	Perform an experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / wireshark / tcpdump
7	Perform an experiment how to use DumpSec.
8	Perform an wireless audit of an access point / router and decrypt WEP and WPA (softwares netstumbler or airsniff)
9	Perform an experiment to sniff traffic using ARP poisoning
10	Install IPCop on a linux system and learn all the function available on the software.
11	Install JCrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management
12	Demonstrate Intrusion Detection System (IDS) using any tool eg. Snort or any other s/w
13	Install RootKits and study variety of opt
14	Generate minimum 10 passwords of length 12 characters using open ssl command
15	Setup a honey pot and monitor the honey pot on network