Program Name	B. Tech. (Computer Engineering)	Semester – VII
Course Code	R4CO4002P	
Course Title	Cyber Security Lab	
Prerequisite	Computer Network	

COURSE OUTCOMES: Students will be able to	
1.	Identify cybercrimes, and respective cyber laws
2.	Build the secure Network infrastructure and reduce the risk of attacks.
3.	Reduce the risk of data theft and web application attacks.
4.	Explore the Security, Defense mechanism And Forensic Best Practices in Advanced domain.

LIST OF EXPERIMENTS: **Hrs CO**

1. **Cyber Crime**

(i)For a given case study on cyber-crime, **2 1**
1.Investigate the Cyber Crimes And evidential aspects.
2.identify the security parameters.
3. Identify the cyber laws for the punishment of **c**ybercrimes and stalking.
Run the following commands on your computer and analyze the results.

1 run c:\> ipconfig/all

2 run c:\> NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

3 ping IP Address

4 tracert type url or IP Address

5. c:\> arp-a

6. Find the open ports using NETWOX tools 67
7.Discuss the following internet address tools

1. Dig
2. Whois
3. Traceroute

8 Enumerate Remote Systems

2. **TCP/IP Security Model** 2 1,2

(i) The TCP/IP STACK deals with the various protocols at various layers of the TCP/IP stack like TCP/IP protocols, routing protocols and security protocols. Study the various protocols, identify vulnerabilities of these protocols and provide the defense mechanism. Identify the tools to do attack and defense mechanism tools.
OR. Download the open-source Linux operating system from the internet and study the code of TCP/IP Model, modify it and embed it in Linux and execute.
(ii) Perform Attacks on Cryptographic Algorithms and Design Robust RSA, DES, Stream Ciphers-RC4 etc. algorithms and implement and test them.

3. **Secure Network Design for Organization** 2 1,2,3

Design the campus wide network for the campus of the engineering college. Analyze The location of the core switch, distribution switch and access switch and departmental requirements for connectivity of the computers. Also specify the requirements for setting the data centre and firewall and IPS, Routing Requirements. Identify active and passive components specifications for the design of the network. Identify the vulnerabilities, attacks and defense mechanism for the security of organization's enterprise network. Formulate the organizational guidelines for network and computing infrastructure usage.

4. **Practical Experiment on Firewall** 2 1,3

(i) Each student shall Download and install each type of open-source firewall, perform the experiment and note the results. Write a report of your experimentations; and check with the domain expert

1. SHORELINE, JAY" S, GUARDDOG firewalls are classified as Packet Filtering firewalls

2 NETNANNY, CYBERPATROL, DANE GUARDIAN and GAUNTLET firewalls are classified as Data Filtering firewalls.

3. IPCOP and SMOOTHWALL firewalls are both Data Filtering as well as Packet Filtering firewalls.

(ii) Study the commercial software's (firewall and IDS) if you have access from any sources Write a report of your experimentations; and check with the domain.

5. **Implement Intrusion Detection Systems**. 2 2

Use the following steps:

1. Capture packets using windup/TCPDump and storing in packet.txt
2. Preprocess packet.txt to give input to the patterning matching algorithm.
3. Storing the normal and abnormal traffic patterns in pattern.txt file. You can use KDD cup data or create your own data for the experiment.
4. Pattern Matching step: if pattern in the pattern.txt file matches with any of the abnormal attack packet in packet.txt file, then the packet is abnormal packet otherwise it is normal packet
5. Display result as normal or abnormal packet (attack or intrusion).

6. **Protocol Analysis Tools.** 2 1,3

Download and install the following packet capture softwares on your computer(any one by each student)

1. Wireshark
2. TCPDUMP
3. WindowDump
4. NMAP

What are the facilities provided by the softwares? Illustrate the features of each softwares? Study and analyse following protocols or any other protocols of your choice.(any two by each students)

(i)ARP (ii) IP (iii) TCP (iv) DNS packet (v) SMTP protocol (vi) BGP

Show the report to your teacher

7. **The Attacks On Web Application and Defense Mechanism** 2 1,3

Consider the systems software's and applications software are loaded on web server, application server and database server. Gather the information about the enterprise for making the attacks. How can you do Top 10 OWASP attack. Apply secure software life cycle for the given case study. Write the secure code and provide the defense mechanism against Top 10 OWASP attack. You can use ESAPI Or Any Other Framework.

8. **Hardening Linux and Database for Cyber Security** 2 2

(i)Harden the Linux operating systems with respect to following
1. Basic security 2. File and directory security 3. Workstation security 4. Server security 5. Network services security
(ii)Perform the experiment for Data base security using RBAC, DAC, MAC and identify the source of unauthorized users accessing the database.
(iii) Identify the organizational Implications for organizational policy, web threats, security and privacy and incident handling

9. Defense Mechanism Against Hackers Methodology. 2 3,4

Illustrate the Hackers methodology with suitable experiment in order to improve the quality of the computing systems services of your organization.
(Hint: Foot printing, Scanning, Enumeration, gaining access, escalating privileges, covering tracks, Creating backdoors, Denial of service)
i) Which techniques and tools are used by the hacker at each phase of hacking of computing assets of your network/laptop/PC?
ii) Perform the experiment for the passive attacks and active attacks on computing systems of your organization's data centre/laptop/PC and show the results to the owner of organization with snapshots.
iii) Suggest the defense mechanism strategy/tools at every phase of hacking in order to protect the computing assets of your data centre.
(iv) Cybercrime: Illustrations and case studies.

10 **GROUP PROJECTS** 2 3

1. Select any group project on following.

Analyze design, implement and Test project (any one)

Modification Of TCP/IP, Network Security, Web Application Security, Secure Life Cycle, Security. E Testing IPS, Firewall, Computer Hacking and Forensic Investigation, Mobile Security, Mobile Forensic, Cloud Security, Cloud Forensic, Security and forensic of Hand-held devices. OR Any Other Project Assigned by Teacher on Cyber Security.

TEXTBOOKS

1. Dr. B.B. Meshram, Ms K.A. Shirsath, "TCP/IP and Network Security: Attacks and Defense Mechanisms with Open-Source Tools", Shroff Publishers & Distributors PVT. LTD, 1st edition, 2017.

2. John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics", Elsevier, 1st Edition, 2012.

RECOMMENDED READING

1 Charles Pfleeger, “Security in Computing”, 4th Edition, Prentice Hall of India, 2006.

2 Roberta Bragg, M.r. Ousley. Keith Strassberg, “Network Security- The Complete Reference”, Tata McGraw-Hill