

NETWORK & CYBER SECURITY

PRACTICAL MANUAL

Submitted By

Biren Hirapara

ENROLLMENT NO. – 235690694010

3RD SEMESTER

SUBJECT CODE – 639410

Of

MASTER OF COMPUTER APPLICATIONS



GOVERNMENT MCA COLLEGE MANINAGAR
(EAST),

AHMEDABAD GUJARAT

[Academic Year: 2024-25]



Government MCA College, Maninagar (East)
K. K. Shastri Educational Campus
Khokhra Road, Ahmedabad – 380008, Gujarat

Date:

CERTIFICATE

This is to certify that Biren Hirapara **(ENROLLMENT**
NO. – 235690694010 **), Student of MCA 3RD Semester, Government MCA College**
has successfully completed his practical work of subject Network & Cyber Security
(639410) for academic year 2024-25.

DATE OF SUBMISSION:

Prof Nisha K. Chavda
Lecturer,
Government MCA College,
Maninagar, Ahmedabad

Prof Bhavesh B. Prajapati
HOD,
Government MCA College,
Maninagar, Ahmedabad

Dr. Chetan B. Bhatt
Principal,
Government MCA College,
Maninagar, Ahmedabad

VISION OF THE INSTITUTE

- Provide value-based quality education for computer science applications which enable students to solve real-life problems of society.

MISSION OF THE INSTITUTE

- To equip our students with good knowledge, skills and attitude to solve real – life problems in the domain of computer applications.
- To establish industry-academia interaction to facilitate the students to work proficiently in the industrial environment.
- To imbibe high moral values and professional ethics.
- To provide conducive environment so as to achieve excellence in teaching-learning, and research and development activities.

PROGRAM EDUCATIONAL OBJECTIVES

- Identify and analyze real life problems and design computing systems appropriate to its solutions that are technically sound, economically feasible and socially acceptable
- Exhibit professionalism, ethical attitude, good communication skills, team work in their profession
- Adapt to current trends by engaging in life-long learning

PROGRAM OUTCOMES (POs)

- ▶ **PO1 (Foundation Knowledge):** Apply knowledge of mathematics, programming logic and coding fundamentals for solution architecture and problem solving.
- ▶ **PO2 (Problem Analysis):** Identify, review, formulate and analyze problems for primarily focusing on customer requirements using critical thinking frameworks.
- ▶ **PO3 (Development of Solutions):** Design, develop and investigate problems with as an innovative approach for solutions incorporating ESG/SDG goals.
- ▶ **PO4 (Modern Tool Usage):** Select, adapt and apply modern computational tools such as development of algorithms with an understanding of the limitations including human biases.
- ▶ **PO5 (Individual and Teamwork):** Function and communicate effectively as an individual or a team leader in diverse and multidisciplinary groups. Use methodologies such as agile.
- ▶ **PO6 (Project Management and Finance):** Use the principles of project management such as scheduling, work breakdown structure and be conversant with the principles of Finance for profitable project management.
- ▶ **PO7 (Ethics):** Commit to professional ethics in managing software projects with financial aspects. Learn to use new technologies for cyber security and insulate customers from malware
- ▶ **PO8 (Life-long learning):** Change management skills and the ability to learn, keep up with contemporary technologies and ways of working.

PROGRAM SPECIFIC OUTCOMES (PSOs)

After completing the program students will be able to

- Meet the needs of users within an organizational and societal context through the selection, creation, application, integration, and administration of computing technologies.
- Apply concepts, probability, statistics, mathematics, through calculus (differential and integral), numerical methods and sciences including applications appropriate in the field of computing problems.
- Use algorithms, data structures, database management, software design, concepts of programming languages and computer organization and architecture in the field of computer applications.

COURSE OUTCOMES (COs)

1. Describe network devices and concepts of network security.
2. Explain concepts and techniques of information security.
3. Illustrate commands for network identification and scanning.
4. Explain ways to monitor and analyze network traffic using Wireshark.
5. Describe concepts of wireless security.
6. Describe network devices, cyber-attacks and network security basics.
7. Perform and analyze the output of network management commands.
8. Use tools related to information and network security.

INDEX

Sr No	Title	Page No	Date	Sign
1	<ul style="list-style-type: none">• To study various attacks based on layers of OSI Model.• To study various wired & wireless network devices based on layers of OSI Model.			
2	<ul style="list-style-type: none">• To study the features of firewall in providing Network Security and policy implementation on any basic firewall.• To implement whitelisting & blacklisting policy in the firewall.			
3	<ul style="list-style-type: none">• To perform various encryption-decryption techniques with cryptool.			
4	<ul style="list-style-type: none">• To Implement Caesar cipher encryption-decryption.• To study SHA-1 hash & digital signature algorithm.			
5	<ul style="list-style-type: none">• To perform Open Source Intelligence (OSINT) about any specific domain. (WHOIS, DNS, Lookup & other Tools) – A Passive Information Gathering Technique.			
6	<ul style="list-style-type: none">• To perform following operations using Netcat: Port Scanning & Port Listening ,Banner Grabbing, File/Data Transfer , Chat Server			
7	<ul style="list-style-type: none">• To Study the use of network reconnaissance tools like ping, traceroute, nslookup to gather information about networks and domain registrars.			
8	<ul style="list-style-type: none">• To perform port scanning using various methods & techniques provided by Nmap or Zenmap.			
9	<ul style="list-style-type: none">• To implement a packet capturing tool (Wireshark) and capture the real time traffic.• To study & analyze the captured packets for different protocols & search queries using Wireshark.• Observe performance in promiscuous as well as non-promiscuous mode in Wireshark and also show that packets can be traced based on different filters.			
10	<ul style="list-style-type: none">• Use the Nessus tool to scan the network for vulnerabilities.• To implement/configure Intrusion Detection System for Log Collection based on default & customized rules. (Ex. Snort IDS)			
11	<ul style="list-style-type: none">• To study ARP Protocol & perform ARP poisoning attack.• To study WEP, WPA2PSK and perform WEP, WPA cracking.			
12	<ul style="list-style-type: none">• To study and report on latest Network Security Crimes, Network Security Challenges and Solutions to overcome them.			