GUJARAT TECHNOLOGICAL UNIVERSITY

Syllabus for Master of Computer Applications, 3rd Semester
Subject Name: Network & Cyber Security
Subject Code: 639410

With effective from academic year 2020-21

1. Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
3	-	2	4	70	30	30	20	150

2. Course Outcomes:

Course Outcome Component	Course Outcome (Learner will be able to)
CO1: Concepts of Network Security	• Learn and describe about various network security and cyber security concepts, devices used to enhance security of networks.
CO2: Concepts of Cryptography and IP Security	• Learn and describe about various cryptographic techniques, digital signatures, various hashing algorithms and their importance and internet protocol architecture.
CO3:Network Scanning and Identification	• Learn and identify various devices present across network, identify the open ports on the active devices, identify the OS information and banner information of various servers and machines.
CO4:Network Monitoring and Analysis	• Learn and capture traffic from the active network, analyse packets & protocols and create their own Network Monitoring System
CO5: Wireless Security	• Learn and describe various security authentications and standards used, detect and mitigate various attacks performed on wireless network infrastructure.

3. Course Duration: The course duration is of **40 sessions of 60 minutes each.**

4. Course Contents:

Module No:	Contents	No. of Sessions	70 Marks (External Evaluation)
I	• **Introduction to Network Security & Cyber Security Concepts:** Network Security and its need, CIA (Confidentiality, Integrity, Availability), AAA (Authentication, Authorization, Accounting), Network Devices (Host, Router, Switch, Bridge, etc..) on Each Layer of OSI Model, Working of DNS, DHCP, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), Firewall and its types, Web Proxies, Internet Security Protocols	6	
II	• **Introduction to Cryptography & IP Security:** Key Terms: Encryption, Decryption, Plain Text, Cipher Text, Secret Code, Types of Cryptographic Functions,	5	

	Secret Key Cryptography, Public Key Cryptography, Hashing, Hash Algorithms, Digital Signatures, IP Security Architecture – Authentication Header, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange (IKE).		
III	• **Network Security Assessment - 1:** Passive Information Gathering: IP Address & Domain Identification, Banner Grabbing (Netcat, Telnet & other tools), Identifying Domain Ownership (WHOIS, DNS Lookup & other tools), Active Information Gathering: Detecting Active Systems, ICMP Ping, Port Scanning and its techniques, Port Scanning Tools (Nmap, Zenmap, Superscan & other tools), OS Fingerprinting – Active & Passive.	11	
IV	• **Network Security Assessment - 2:** Physical Interception, Traffic Capturing Tools (Wireshark), Packet Analysis, Protocol Analysis, Traffic Timeline Analysis, Setting up your own Network Intrusion Detection System (SNORT-NIDS).	10	
V	• **Wireless Security:** Wi-Fi basics – Wireless Clients and NICs, Wireless Access Points (WAP), Wireless Communication Standards, Wi-Fi Security – 802.1x Authentication, Wireless LAN Threats – Wardriving (NetStumbler, Kismet), Eavesdropping, Rogue and Unauthorized Access Points, Evil Twin Attack, DOS, WLAN Encrytion Flaws: Cracking WPA/WPA2 PSK, Decrypting WEP and WPA Packets, ARP poising and MAC spoofing, Security Wireless Security.	8	

5. Pedagogy:

- ICT enabled Classroom teaching
- Case study
- Practical / live assignment
- Interactive class room discussions

6. Evaluation:

Students shall be evaluated on the following components:

A	**Internal Evaluation**	**(Total - 20 Marks)**
	• Continuous Evaluation Component	10 marks
	• Class Presence & Participation	10 marks
B	**Mid-Semester examination**	**(30 Marks)**
C	**End –Semester Examination(Theory)**	**(70 Marks)**
D	**End –Semester Examination(Practical/Viva)**	**(30 Marks)**

7. Reference Books:

No.	Author	Name of the Book	Publisher

1.	Micheal Gregg	Build Your Own Security Lab: A Field Guide for Network Testing	Wiley Publishing
2.	Charlie Kaufman, Radia Perlman and Mike Speciner	Network Security: Private Communication in a Public World	Pearson Indian Education Services Ltd.
3	William Stallings	Cryptography and Network Security: Principles and Practice	Pearson
4.	Lisa Bock	Learn Wireshark	Packt Publishing
5.	Nicholas Marsh	Nmap® Cookbook: The Fat-Free Guide to Network Scanning	Createspace Independent Pub
6.	ED Wilson	Networking Monitoring And Analysis : A Protocol Approach to Troubleshooting	Prentice Hall PTR
7.	Chris McNab	Network Security Assessment: Know your Network	O'Reilly