AC– 11-03-2025
Item No. – 05

Approved by the BoS in Information Technology on
05-03-2025 Item No. 05

As Per NEP 2020

Tolani College of Commerce (Autonomous)

Title of the Course: Security in Computing

Programme: B.Sc.(Information Technology) Semester VI

Syllabus for 2 credits

From the academic year-2024-2025

Sr. No.	Heading	Particulars
1	**Description the course :**	Information security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication. Network security is concerned with protecting data, hardware, and software on a computer network.
2	**Vertical:**	Major
3	**Type:**	Theory and Practical
4	**Credit**:	4 credits
5	**Hours Allotted:**	60 Hours
6	**Marks Allotted**:	100 Marks Continuous Evaluation: 40Marks Semester-End: 60 Marks
7	**Course Objectives** **1.** Equip students with a foundational knowledge of key security principles, including confidentiality, integrity, availability, and authentication. **2.** Enable students to identify various types of security threats and vulnerabilities in computing environments and to assess risks to develop effective mitigation strategies. **3.** Teach students how to implement and configure security measures, such as encryption, firewalls, and intrusion detection systems, to protect information systems. **4.** Explore the legal and ethical implications of computing security, including data privacy regulations and ethical hacking practices.	
8	**Course Outcomes**: 1. Students are able to explain the core concepts of confidentiality, integrity, availability, and authentication in the context of computing systems. 2. Students can successfully identify common security threats and vulnerabilities in various computing environments through practical assessments. 3. Students can demonstrate proficiency in configuring and deploying security technologies, such as encryption protocols and firewall settings, in lab environments. 4. Students can analyze real-world scenarios involving ethical dilemmas in security practices and propose responsible solutions.	

9	**Modules**:-
	Module1:Information Security, Risk Analysis, **Secure Design Principles (15 Hours)**
	• The Importance of Information Protection, The Evolution of Information Security, Justifying Security Investment, Security Methodology, How to Build a Security Program, The Impossible Job, The Weakest Link, Strategy and Tactics, Business Processes vs. Technical Controls. • Threat Definition, Types of Attacks, Risk Analysis. • The CIA Triad and Other Models, Defense Models, Zones of Trust, Best Practices for Network Defense
	Module2:Authentication and Authorization, Encryption, **Storage Security, Database Security**: **(15 Hours)**
	• Authentication, Authorization • A Brief History of Encryption, Symmetric-Key Cryptography, Public Key Cryptography, Public Key Infrastructure. • Storage Security Evolution, Modern Storage Security, Risk Remediation, Best Practices. • General Database Security Concepts, Understanding Database Security Layers, Understanding Database- Level Security, Using Application Security, Database Backup and Recovery, Keeping Your Servers Up to Date, Database Auditing and Monitoring.
	Module3:**Secure Network Design, Network Device Security**, **Firewalls, Security Models (15 Hours)**
	• Introduction to Secure Network Design, Performance, Availability, Security. • Switch and Router Basics, Network Hardening. • Overview, The Evolution of Firewalls, Core Firewall Functions, Additional Firewall Capabilities, Firewall Design. • Classic Security Models, Reference Monitor, Trustworthy Computing, International Standards for Operating System Security
	Module4:**Intrusion Detection and Prevention Systems , Virtual Machines and Cloud Computing**, **Secure Application Design, Physical Security (15 Hours)**
	• IDS Concepts, IDS Types and Detection Models, IDS Features, IDS Deployment Considerations, Security Information and Event Management (SIEM). • Virtual Machines, Cloud Computing. • Secure Development Lifecycle, Application Security Practices, Web Application Security, Client Application Security, Remote Administration Security. • Classification of Assets, Physical Vulnerability Assessment, Choosing Site Location for Security, Securing Assets: • Locks and Entry Controls, Physical Intrusion Detection.

11	**Reference Books:** 1. **Author:** Mark Rhodes- Ousley, **Title:** The Complete Reference: Information Security, **Publisher:** McGraw- Hill 2nd Edition**year**:2013 2. **Author:** Josiah Dykstra **Title:** Essential Cybersecurity Science, **Publisher:** O'Reilly 5th Edition **year**:2017 3. **Author:** Wm. Arthur Conklin, GregWhite **Title:** Principles of Computer Security: CompTIA Security+ and Beyond, **Publisher:** McGraw Hill2nd Edition **year**:2010

12	**Internal Continuous Assessment:40%**	**Semester End Examination:60%**
13	**Continuous Evaluation through:**	**Practical**

14 **Format of Question Paper:**

Scheme of Evaluation Pattern

Table 1A: Scheme of Continuous Evaluation (CE)
Scheme of Evaluation Pattern

Sub-components	Maximum Marks	Conditions for passing
1)Practical exam	30	A learner must be present for each of the sub components
2)Journal and Viva	10	
Total	40	

Table1B:SchemeofSemesterEndExamination(SEE)Evaluation Question Paper Pattern for Semester End Examination (SEE)

Maximum Marks: 60 **Duration:2 Hrs.**

Note: All questions are compulsory .Each question has an internal choice.

Q.1.		Attempt any two of the following	15
	a)		
	b)		
	c)		
	d)		
	e)		
		Attempt any two of the following	15
Q.2.	**a)**		
	b)		
	c)		
	d)		
	e)		
		Attempt any two of the following	15
Q.3.	**a)**		
	b)		
	c)		
	d)		
	e)		
		Attempt any two of the following	15
Q.4.	**a)**		
	b)		
	c)		
	d)		
	e)		

Course Name: Security in Computing Practical			
Periods per week (1 Period is 60 minutes)		**4**	
Credits		**2**	
		Hours	**Marks**
Evaluation System	**Practical Examination**	**2**	**40**

Practical No	Details
1	**Configure Routers**
a	OSPF MD5 authentication.
b	NTP.
c	to log messages to the syslog server.
d	to support SSH connections.
2	**Configure AAA Authentication**
a	Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA
b	Verify local AAA authentication from the Router console and the PC-A client
3	**Configuring Extended ACLs**
a	**Configure, Apply and Verify an Extended Numbered ACL**
4	**Configure IP ACLs to Mitigate Attacks and IPV6 ACLs**
a	Verify connectivity among devices before firewall configuration.
b	Use ACLs to ensure remote access to the routers is available only from management station PC-C.
c	Configure ACLs on to mitigate attacks.
d	Configuring IPv6 ACLs
5	**Configuring a Zone-Based Policy Firewall**
6	Configure IOS Intrusion Prevention System (IPS) Using the CLI
a	Enable IOS IPS.
b	Modify an IPS signature.
7	**Layer 2 Security**
a	Assign the Central switch as the root bridge.
b	Secure spanning-tree parameters to prevent STP manipulation attacks.
c	Enable port security to prevent CAM table overflow attacks.
8	**Layer 2 VLAN Security**
9	**Configure and Verify a Site-to-Site IPsec VPN Using CLI**

1	Q.1	15
2	Q.2	15
3	Viva	5
4	Journal	5
5	**Total**	**40**