Cyber Security

Government of Karnataka

DEPARTMENT OF COLLEGIATE and TECHNICAL EDUCATION

Program	**Computer Science & Engineering**	**Semester**	**5**
Course Code	**20CS54I**	**Type of Course**	**L:T:P (104:52:312)**
Course Name	**Cyber Security**	**Credits**	**24**
CIE Marks	**240**	**SEE Marks**	**160**

Introduction:

Welcome to the curriculum for the Artificial Intelligence and Machine Learning (AI&ML) Specialisation. This specialisation course is taught in Bootcamp mode. Bootcamps are 13 weeks, intense learning sessions designed to prepare you for the practical world – ready for either industry or becoming an entrepreneur. You will be assisted through the course, with development-based assessments to enable progressive learning.

In the era of connected computing devices, securing the personal data, application, system, network and organization becomes the challenging task in the field of Computer science and Engineering. The specialization prepare students to take up job or to become entrepreneur in the challenging area of Cyber security

Pre-requisite

Before the start of this specialisation course, you would have completed the following courses;

In the 1st year of study, you would have studied Engineering Mathematics, Communication Skills, Computer Aided Engineering Graphics, Statistics & Analysis, Basic IT Skills, Fundamentals of Computer, Fundamentals of Electrical and Electronics Engineering, Project Management skills and Multimedia & Animation.

In the 2nd year of study, you would have studied Python Programming, Computer Hardware, Maintenance and Administration, Computer Networks, Database System Concepts and PL/SQL, Data Structures with Python, Operating System and Administration, Object oriented programming and Design with Java, Software Engineering principles and practices.

In this year of study, you shall be applying your previous years learning along with specialised field of study into projects and real-world applications.

Course Cohort Owner

A Course Cohort Owner is a faculty from the core discipline, who is fully responsible for one specialised field of study and the cohort of students who have chosen to study that specialised field of study.

Guidelines for Cohort Owner

1. Each Specialized field of study is restricted to a Cohort of 20 students which could include students from other relevant programs.
2. One faculty from the Core Discipline shall be the Cohort Owner, who for teaching and learning in allied disciplines can work with faculty from other disciplines or industry experts.
3. The course shall be delivered in boot camp mode spanning over 12 weeks of study, weekly developmental assessments and culminating in a mini capstone.
4. The industry session shall be addressed by industry subject experts (in contact mode/online / recorded video mode) in the discipline only.
5. The cohort owner shall be responsible to identify experts from the relevant field and organize industry session as per schedule.
6. Cohort owner shall plan and accompany the cohort for any industrial visits.
7. Cohort owner shall maintain and document industrial assignments, weekly assessments, practices and mini project.
8. The cohort owner shall coordinate with faculties across programs needed for their course to ensure seamless delivery as per time table
9. The cohort owner along with classroom sessions can augment or use supplementally teaching and learning opportunities including good quality online courses available on platforms like Karnataka LMS, Infosys Springboard, NPTEL, Unacademy, SWAYAM , etc.

Course outcome: A student should be able to

CO1	Design, optimize, operate and maintain a secure network/system/application/cloud and data resources for given requirements
CO2	Apply cryptography to secure a cyber system.
CO3	Respond to incidents to mitigate immediate and potential threats .
CO4	Test, implement, deploy, maintain and review the infrastructure to effectively manage the network and resources.
CO5	Monitor network to actively remediate unauthorized activities.

Detailed course plan

Week	CO	PO	Days	1st session (9am to 1 pm)	L	T	P	2ND session (1.30pm to 4.30pm)	L	T	P
1	1	1	1	- Protecting your personal data - Online identity - Where is your data ? - Smart devices - What do attackers want ? - Identity theft - Protecting your organization data - Traditional data - Cloud; IoT; Big data - Types of data - Sensitive and non sensitive data - Personal data, PII data - Data classification - Ex: Govt. of India classification of data - Unclassified - Restricted - Confidential - Secret - Top secret -	4	-	-	Introduction and Basic concepts of cyber security What is Cyber security, Security principles CIA, AAA Vulnerability, Threat, Risk, attack and Impact People, Process and Technology McCumbers Cube Cyber Security - Brief history and types - Infrastructure, network, cloud, IOT, application. - Purpose and Importance - Challenges - Applications How does cyber security work?	3		

	1	1,5	2	Recap – Topology OSI Model TCP/IP Model Internet protocols Network resources Router and Firewall, Hub, switch – security issues Basic Network terminologies	3		1	Hackers Who are they? What is not hacking Types of hackers Hacking methodologies Purpose Activity: Stuxnet - a case study	1		2
	1,2, 3	1,2, 3	3	Analysing a Cyber Attack Types of Malwares Spyware Malware Backdoor Ransomware Scareware Rootkit Virus Trojan horse Worms Symptoms of attack Methods of Infiltration Social Engineering Pretexting Tailgating Something for something (quid pro quo) Denial-of-Service and DDoS Botnet On the Path attack	3	1		- Defence in depth - What is defence in depth - Layers - Needs for Defence in depth - Examples - Host encryption - Anti-virus - Firewall - E-Mail gateway - Password management - Honeypot - Multi Factor Auth			3

				SEO Poisoning Wi-Fi Password Cracking Password Attacks Password spraying Dictionary attack Brute force Password Cracking Times Rainbow Traffic interception Advanced Persistent Threats Security Vulnerability and Exploits Hardware Vulnerabilities Meltdown and Spectre Software Vulnerabilities Categorizing Software Vulnerabilities Software updates							
	1,2, 3	1,2, 3	4	Data Maintenance Using free tools Back Up Your Data How Do You Delete Your Data Permanently? Tools Who owns your data? Terms of service Understand the term; what are you agreeing to? The data use policy Privacy settings Before you sign up protect your data Activity: Check terms of service of the popular application you use on your phone and check their data sharing policy, access to device etc.	2	1	1	Protecting Your Computing Devices turn the firewall on install antivirus and antispyware manage your operating system and browser set up password protection.			3

				Safeguarding Your Online Privacy Two Factor Authentication Open Authorization Social Sharing Email and Web Browser Privacy **Activity:** Discover your own risky online behaviour Scenario **1:** posting private info on social media Scenario **2:** What password you choose when creating new account for social service Scenario **3:** Using public Wi-Fi - Scenario **4:** Using trial version of the software **Activity:** Check if your password is compromised Note :Use Have I been pwned -							
			5	**Developmental Assessment**				Assessment Review and corrective action			3
	1,2	2,3, 4	6	**class: Cyber security at workplace**	2		3	Weekly Assignment(1PM-2PM)			
Reference materials : skillsforall.com – Introduction to Cyber security											
2	1,2, 3,4	2,3, 4	1	Peer review Project / activity Propose problem statement		4		Why Do We Need a Version Control System? Fundamentals of Git Git installation and setup basic local Git operations ▪ creating a repository,	1		2

								▪ cloning a repository, ▪ making and recording changes ▪ staging and committing changes, ▪ viewing the history of all the changes undoing changes			
	2,3	2,3, 4	2	History of cryptography (overview: Caesar cipher, enigma cipher) Introduction (high level overview only) Enc (sym - stream + block ciphers, asym) Hashing Digital signature, MAC - PRNG	2		2	Algebra: groups, rings, fields - definitions + examples AES (SPN structure, rounds, modes of operation - high level overview with diagram) MAC + SHA2/3 (high level + security requirements))	1		2
	2,3	2,3, 4	3	RSA (with numerical examples) Digital signature (RSA)	2		2	Number theory - primes, modular arithmetic, gcd, Euler totient function - definitions + examples	1		2
	2,3	2,3, 4	4	Practice sessions/ student activities: - Numerical/programming exercises: subset of math / Caesar cipher / one time pad / RSA / GCD / primality Cryptanalysis (brute force over keys, birthday attacks on hash functions, hardness of	1		3	Practice sessions/ student activities: Inspect digital certificates using a web browser and visiting popular websites - Identify the crypto algorithms in TLS - Design a toy crypto algorithm like key generation + encryption + decryption / digital signature / hash function			3

				factoring integers, discrete log problem, side-channel attacks – high level overview) Applied crypto (PKI, Full disk encryption, blockchain: overview							
			5	**Developmental Assessment**				Assessment Review and corrective action			3
			6	**Industrial class : Application of cryptography**	2		3	Weekly Assignment			

References :

- https://www.youtube.com/user/Computerphile - YouTube channel by Dr. Mike Pound
- https://nptel.ac.in/courses/106105031/ : Cryptography and Network Security by Prof. Debdeep Mukhopadhyay, IIT Kharagpur
- https://www.coursera.org/learn/crypto and https://www.coursera.org/learn/crypto2 : by Prof. Dan Boneh, Stanford University
- http://williamstallings.com/Cryptography/ - student resources by Prof. William Stallings

3	1,4	2,3, 4	1	Peer review Project / activity Propose problem statement and network design requirements		4		How Internet/Application works (Security aspects – end-to-end packet path) Network architecture concepts Understanding vulnerabilities in different OSI layers and protocols (TCP, UDP, IP, ICMP)			3

	1,5	2,3, 4	2	Network Security : Concepts- Firewall, IDS, IPS, VPN	2		2	Protocols : IPSec, SSL, TLS (versions and vulnerabilities)	1		2
	1,5	1,4	3	Web Security : Concepts-HTTP, HTML, Frames, browser design	2		2	Attacks and vulnerabilities: Injection attacks : SQL, HTTP header, OS command	1		2
	1,5	2,3, 4	4	○ Wireless Security : Introduction to security issues in cellular networks, WIFI, LAN systems, RFID systems	2		2	- DOS attacks, countermeasures (in relation to wireless networks)	1		2
			5	**CIE 1 : Written and practice test**				Assessment Review and corrective action			3
	2,3	2,3, 4	6	**Industrial class** : High availability and load balancing	2		3	Weekly Assignment			

References :

1. https://www.cisco.com/c/en_in/products/security/what-is-network-security.html
2. https://purplesec.us/firewall-penetration-testing/
3. How hackers do it: Tricks, Tools, and Techniques
4. https://cse29-iiith.vlabs.ac.in/
5. https://nptel.ac.in/courses/106105031/ : Cryptography and Network Security by Prof. Debdeep Mukhopadhyay, IIT Kharagpur.
6. https://wiki.apnictraining.net/netsec-20220627-bdnog14/agenda

4	2,3, 5	2,3, 4	1	Peer review Project status review Demonstration of artifacts of the project		4		Windows Security Windows Security Infrastructure Windows Family of Products Windows Workgroups and Accounts Windows Active Directory and Group Policy	2		1

	1,2, 3,5	2,3, 4	2	Windows as a Service End of Support Servicing Channels Windows Update Windows Server Update Services Windows Autopilot Windows Virtual Desktop Third-Party Patch Management Practice : Process observation and analysis with Process Hacker	2		2	Windows Access Controls NTFS Permissions Shared Folder Permissions Registry Key Permissions Active Directory Permissions Privileges BitLocker Drive Encryption Secure Boot - Practice : NTFS file system practical using NTFS Permissions Reporter	1		2
	1,2, 3,5	2,3, 4	3	Enforcing Security Policy Applying Security Templates Employing the Security Configuration and Analysis Snap-in Understanding Local Group Policy Objects Understanding Domain Group Policy Objects Administrative Users Privileged Account Management Reduction of Administrative Privileges AppLocker User Account Control Windows Firewall IPsec Authentication and Encryption	2		2	Linux Security Linux Fundamentals Operating System Comparison Linux Vulnerabilities Linux Operating System Shell Kernel Filesystem Linux Unified Key Setup Linux Security Permissions Linux User Accounts Pluggable Authentication Modules Built-in Command-Line Capability	1		2

				Remote Desktop Services Recommended GPO Settings. Practice : Auditing and enforcement of system baseline configurations with security templates PowerShell scripting and automation techniques				Service Hardening Package Management			
	1,2, 3,5	2,3, 4	4	Linux Security Enhancements and Infrastructure Operating System Enhancements ○ SE Linux ○ App Armor Linux Hardening ○ Address Space Layout Randomization ○ Kernel Module Security ○ SSH Hardening ○ Open SCAP ○ CIS Hardening Guides and Utilities	2		2	Log Files ○ Key Log Files ○ Syslog ○ Syslog Security ○ Log Rotation ○ Centralized ○ Logging ○ Audit id ○ Firewalls: Network and Endpoint ○ Rootkit Detection	1		2
			5	**Development Assessment** (Hardening the image win and linux CIS controls)				Assessment Review and corrective action			3
	1,2, 3,5	2,3, 4	6	Industrial Class : System Security	2		3	Weekly Assignment			
5	1,2, 3,4, 5	2,3, 4	1	Peer review Project status review		4		Introduction to Application Security Secure SDLC	2		1

				Introduction to Software Application Development – How was it created, Why is it important? How does it work. Types of Application Software – Thick Client, Web Applications, Web Services, RESTFul Services, Middle Ware, Mobile Applications etc (Give an example of each). Explain Software Development Lifecycle – Requirements, Design, Develop, Deploy, Operate and Purge. Life Cycle Models – Waterfall, Agile, Iterative etc. SDLC Best Practices				Provide a use case – Microsoft Secure SDLC Practice and Security controls covered in each stage at a higher level. Requirements (Determine Application Risk Profile based on Security Requirements, Determine Control Requirements, Establish Quality Gates) b. Design (Architecture Design Review and Threat Modeling) c. Implementation (Static Analysis, Software Composition Analysis, Secret Detection, Deprecate unsafe functions, use of plugins in IDE, Safe Commit and Change Management in Repositories) d. Verification (Dynamic Analysis, Interactive Application Security Testing, Fuzz Testing, Abuse use case Testing, Architecture Verification). e. Release (Run Time Application Self Protection, Web Application Firewall, SOP for Operations, Secure Provisioning, Deployment and De commissioning) - f. Response (Incident Response).			

	1,3, 4,5	2,3, 4	2	Application Security – Requirements 1. Functional and Non Functional Requirements for an application 2. Security Requirements for an application 3. Determining Application Risk Profile Based on the security requirements. 4. Determining Control Requirements Based on Application Risk Profile and Eligibility Criteria for an application to undergo a certain security control. Establish Security Toll Gates	1		3	Application Security Design: Secure Architecture Review – For a given use case, with examples; conduct security architecture review using the OWASP standard.	1		2
	1,3, 4,5	2,3, 4	3	Application Security Design – Threat Modelling. 1. Why Threat Modelling 2. What is Threat Modelling 3. Threat Modelling Methodologies – STRIDE, PASTA, OCTAVE, TRIKE, VAST. 4. Threat Model Ranking – DREAD, CVSS, CWSS etc. Threat Model Execution Phases: - Planning, Scoping, Deep Dive Discussions, Drawing a	1		3	- Using the Microsoft Threat Modeling methodology, execute a threat model for a given application architecture using Microsoft threat modeling tool.			3

				Threat Model, Identifying Threats, Threat Objects, Security Controls, Threat Actors, Threat Traceability Matrix, Reporting and Debrief.							
	1,3, 4,5	2,3, 4	4	Application Security – Implementation - Explain use of Security Tools within IDE. - Static Code Analysis Tools – Explain with examples. - Explain Software Composition Analysis, Identifying Software Dependencies and CVE in underlying libraries. Demonstrate a tool like OWASP Dependency Check.	1		3	Explain Secret Detection using tools like Githound. - Change Management during pre-commit and post-commit in repositories. - Safe SCM practices (Take Github as an example). - Highlight deprecated unsafe functions in common programming languages.			3
			5	**CIE 2 – Written and Practice Test**				Assessment Review and corrective action			3
	1,2, 3,4, 5	2,3, 4	6	**Industrial class : Source Code Scan using a commercial tool like Microfocus Fortify or Checkmarz.**	2		3	Weekly Assignment			
6	1,2, 3,5	2,3, 4	1	Peer review Project status review		4		Application Security – Verification. Explain Dynamic Analysis using an example – owasp zap. Interactive Application Security Testing – Demonstrate using Contrast Security Tool.			3

	2,3, 5	2,3, 4	2	For a given site (local), conduct a dynamic analysis scan using OWASP ZAP, Check for False positives and create a report			4	Introduce Manual Security Testing using OWASP Testing Guide. Add Misuse case testing to the framework in addition	1		2
	2,3, 5	2,3, 4	3	Conduct a manual security testing for a local web application or an API using proxy tools like burp suite/paros etc and provide a report. Compare the results of both manual and automated scans. Application Security – Release 1. Explain Run Time Application Self Protection – Contrast Security or Microfocus Fortify Software can be used as an example. 2. Define Web Application Firewall. Demonstrate using a tool. Elaborate on Standard Operating Procedure for Operations, Secure Provisioning, deployment and decommissioning	1		3	- 1. Cover OWASP ASVS and its aid as a tool in architecture verification. Introduce OWASP SAMM – to attain software assurance maturity.	1		2
	2,3, 5	2,3, 4	4	Measurement of Application Security – Define Metrics, Type of Metrics (Operations, Efficiency, Quality etc). Example Application Security Metrics from OWASP.	1		3	For the previous run scans, define metrics and evaluate the values at operational level.			3

			5	**Development assessment**				Assessment Review and corrective action			3
	2,3, 5	2,3, 4	6	**Industrial class : Dynamic Analysis using Qualys**				Weekly Assignment Weekly Assignment (Suggestive Student Activities) 1. Install Web Goat and do an automated scan using one of the dynamic analysis tools. 2. Follow up with a manual security testing with OWASP Testing guide as an aid and compare the results of automated and dynamic scan.			

References:
1. https://www.synopsys.com/glossary/what-is-sdlc.html
2. https://www.synopsys.com/blogs/software-security/secure-sdlc/
3. https://www.microsoft.com/en-us/securityengineering/sdl
4. https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
5. https://www.microsoft.com/en-in/download/details.aspx?id=49168
6. https://medium.com/@melsatar/software-development-life-cycle-models-and-methodologies-297cfe616a3a
7. https://owasp.org/www-project-application-security-verification-standard/
8. https://resources.infosecinstitute.com/topic/application-architecture-review/
9. https://owasp.org/www-community/controls/Static_Code_Analysis
10. https://owasp.org/www-project-web-security-testing-guide/
11. https://owasp.org/www-project-zap/
12. https://owasp.org/www-project-dependency-check/
13. https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
14. https://owasp.org/www-project-samm/
15. https://github.com/tillson/git-hound
16. https://owasp.org/www-project-security-qualitative-metrics/
17. https://www.qualys.com/apps/web-app-scanning/
18. https://www.veracode.com/security/interactive-application-security-testing-iast
19. https://en.wikipedia.org/wiki/Runtime_application_self-protection
20. https://en.wikipedia.org/wiki/ModSecurity

21.	https://github.com/WebGoat/WebGoat										
22.	https://spectralops.io/resources/how-to-choose-a-secret-scanning-solution-to-protect-credentials-in-your-code/										
23.	https://www.geeksforgeeks.org/functional-vs-non-functional-requirements/										
24.	https://owaspsamm.org/model/design/threat-assessment/stream-a/										
25.	https://docs.42crunch.com/latest/content/concepts/security_quality_gates.htm										
7	1,3, 4	2,3, 4	1	Peer review Project status review		4		Basics of cloud computing Why is cloud computing necessary? Introduction to key cloud services (Compute, storage, networking) Cloud delivery models IaaS v/s PaaS v/s SaaS Introduction to cloud vendors(Azure,AWS, GCP) Key Cloud Security Principles Shared responsibility model Principle of least privilege Defense in depth Threat actors, diagrams & trust boundaries Practice : Create a cloud account Create 2 accounts Setup 2Factor Authentication on both account			3
	1,3, 4	2,3, 4	2	Cloud asset management	1		3	Identity & Access management in the cloud Introduction to IAM Introduction to Federal Identity Management IAM Best Practices			3

								IAM Audit Intro to AWS/Azure clint and Web Portal			
	3,4	2,3, 4	3	Vulnerability management Discovering cloud misconfiguration Remediating vulnerabilities Tracking open vulnerabilities using cloud native tools	1		3	Network security Security groups VPC WAF	1		2
	3,4	2,3, 4	4	Incident response - Log analysis - Events & alerts - Key metrics (MTTD & MTTR)	1		3	Data protection in the cloud • Data protection at rest and at transit • Cloud data storage - AWS EBS, S3 / Azure SAS • Secrets Management			3
			5	**CIE 3 – Written and Practice Test** **Secure a vulnerable cloud env**				Assessment Review and corrective action			3
	3,4	2,3, 4	6	**Industrial class :** **1. Preventing DDoS in a cloud native env** **Hybrid cloud env**	2		3	Weekly Assignment			
8	1,3, 4,5	2,3, 4	1	Peer review Project status review		4		Intro to VAPT Developing a Hacker Mindset • Ethics of Penetration Testing • Goal of Penetration Testing • Thinking like a Hacker • ATT&CK Framework Overview • Introduction to the framework • Deep dive into the key topics	1		2

								○ Reconnaissance ○ Initial Access ○ Privilege Escalation ○ Lateral Movement ○ Exfiltration			
	1,3, 4,5	2,3, 4	2	Web Application Penetration Testing • Basics of Web ○ HTTP Methods ○ HTTP Requests & Response ○ Session management & Cookies			4	Web Application Penetration Testing • Finding common web vulnerabilities (OWASP top 10) • Burp Suite Essentials Practical:Setup Burp Suite on local machine and observe traffic of 1 website..			3
	1,3, 4,5	2,3, 4	3	Cloud Penetration Testing • Finding common cloud vulnerabilities • Introduction to tools: Nessus, NMAP, Prowler			4	Introduction to OSINT: • Scanning the internet (example: Shodan) • Google dorking • Subdomain enumeration & asset monitoring			3
	1,3, 4,5	2,3, 4	4	Hands-on exercise 1: Complete 3 server-side and 3 client-side topic from Burp Suite academy: https://portswigger.net/web-security/learning-path	1		3	Hands-on exercise 2: Complete either the attacker or defender track in http://flaws2.cloud	1		2
			5	**Developmental Assessment**				Assessment Review and corrective action			3
	1,3, 4,5	2,3, 4	6	**Industrial class :** How penetration testing is used in companies to improve their Security posture				Weekly Assignment			

9	1,3, 4,5	2,3, 4	1	Peer review Project status review		4		Mobile Application Security Testing ○ Basics of Mobile Application ○ Introduction to Android Mobile OS ○ Understanding Android Security Architecture ○ Introduction to iOS Mobile OS ○ Understanding iOS Security Architecture	1		2
	1,3, 4,5	2,3, 4, 7	2	Understanding Android Application security • Reversing Android Application Package • Analysing Android Application Certificates and Signatures • Verifying Android Application Signatures • Analysing the Android Manifest file	1		3	Setting up the environment: • Installing Android Studio • Installing Geny Motion Emulator (Free) • Creating Android Virtual Devices • Using Android Debug Bridge (ADB) to interact with the Android Virtual Devices (AVD) • Transferring files between Host machine and AVD using ADB • Installing Android Applications onto AVD via ADB	1		2
	1,3, 4,5	2,3, 4, 7	3	Setup the following tools onto your machine and reverse the application on the DIVA Android application. - Apktool			4	Mobile Application Security Testing • Introduction to Mobile OWASP Top 10 • Burp Suite/OWASP Zap for Mobile Applications	1		2

				- Dex2Jar - JDGUI							
	1,3, 4,5	2,3, 4	4	Setting up for Android Application Security Testing Install DIVA Android Application (https://github.com/payatu/diva-android) ● Mobile Security Exploitation ● Exploiting Insecure Data Storage ● Exploiting Insecure Cryptographic Implementations ● Exploiting Data Leakage Vulnerabilities	1		3	Exercise: Setup MobSF locally on your system and scan any 5 Android Applications.	1		2
			5	**CIE 4 – Written and Practice Test**				Assessment Review and corrective action			3
	1,3, 4,5	2,3, 4	6	**Industrial class :** Bug bounty hunting				Weekly Assignment			

References :

1. **Basics of Web: https://www.hacker101.com/sessions/web_in_depth.html**
2. **NMAP Basics: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/**
3. **HTTP Proxy:**
    a. **Burp Suite Essentials: https://www.youtube.com/playlist?list=PLoX0sUafNGbH9bmbIANk3D50FNUmuJIF3**
    b. **OWASP Zed Attack Proxy: https://www.zaproxy.org/getting-started/**
4. **Vulnerability Scanning with Nessus: https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus**

5. **How to think like a Hacker: https://www.darkreading.com/vulnerabilities-threats/how-to-think-like-a-hacker**

The Cuckoo's egg (book)

10	3,4	2,3, 4, 7	1	Peer review Project status review		4		Incident management introduction and objectives Stages and life cycle of incident management Tracking incidents Incident remediation Reporting and documentation Incident Closure Incident management teams and models Incident management services and integration tools - Best practices of Incident Management	1		2
	3,4	2,3, 4, 7	2	Fundamentals · CIA · Threat Actors · Different kinds of hackers · Different kinds of teams – Blue, Red, Purple · Criminal Groups · Hactivist Groups · APT · Attack Vectors · Protect/Prevent · Detect/Respond · Trust Positive vs False Positive Data · Bits and Bytes	1		3	Network · Quick revision of OSI model, encapsulation, IP, Subnets, TCP/UDP, well known ports, TCP/IP, Layer 2 Network Protocols · Quick revision of SMTP, HTTP, HTRPS/TLS, DNS Web technologies · Quick revision of DOM, CSS, Javascript, Ajax, MVC, Databases, SQL Authentical protocols	1		2

				· Charter Encoding (ASCII, UTF-8,Base64) · File Magic Bytes, Hashes · Imphash · Ssdeep Windows & Linux - · Quick revision on basic commands, important files and directories, windows registry and processes, Audit in Linux				· Quick revision of Kerberos, SAML, OpenID, OAuth			
	3,4	2,3, 4	3	Understanding the tools and products used in any organization · Firewall, load balancers, proxy, email infrastructure, IDS, DNS, Ani-virus, Content Delivery Solutions, Malware Protection System, Endpoint Detection and Response, Network Access Control, Placement of all devices in the organization – Tier1, Tier 2, Tier 3, DMZ	1		3	Continued..			3
	3,4	2,3, 4	4	SIEM · Understanding logs · Email, Proxy, DNS, IDS, Firewall, AV, EDR, Web application, Unix, Windows Attack Types/Vectors · Phishing, Malware, Distributed Denial of Service, Vulnerabilities (Infrastructure, Application, third party), Web attacks, Misconfigurations, Brute force	1		3	Basics of Incident Response · Alert processing · Procedures, runbooks and reference · Response options · Escalations · Incident categories · Incident Resolution Codes Data Analysis			3

				Attack Models · The cyber kill chain, MITRE ATT&CK Framework, Pyramid of Pain				· Data vs Intelligence · Indicators of compromise (IoCs) · Malware analysis · Accessing IoCs · Contacting threat intelligence Analysis tools · Anomaly · Domain tools · WhoIS · Passive DNS · Virus total · Dynamic File analysis			
			5	**Developmental Assessment**				Assessment Review and corrective action			3
	3,4	2,3, 4, 7	6	**Industrial class :** Handling Internal and external incidents Complexity of Incident management Demo of real world SOC				Weekly Assignment			

References :

1. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

2. https://www.cisa.gov/uscert/bsi/articles/best-practices/incident-management

https://www.infotech.com/research/ss/develop-and-implement-a-security-incident-management-program

Lab : https://letsdefend.io

11	3,4, 5	2,3, 4	1	Peer review Project status review		4		GRC (a) 1) Definition of GRC, introduction to IT governance (b) 2) Importance of GRC in cyber security (c) 3) Policies, processes and procedures (d) 4) Importance of checklists, templates and guidelines Enterprise risk management (a) Understanding risks that enterprises face – Operational Risks, Strategy Risks, Credit risks, Reputational risk, Market risks, Cyber risk (b) Cyber risk integration with Operational risk management	1		2
	3,4, 5	2,3, 4,7	2	- <u>Introduction to basics of risk management</u> Probability, Impact:-- [Financial, Legal, Regulatory, Reputational], Threat, Risk Assessment, Risk Treatment:-- [Accept, Mitigate, Transfer, Avoid], Residual risk, risk acceptance, Control objective, Controls:-- Preventive control, detective control and corrective control	1		3	<u>Patch management</u> Importance of patch management; pre-requisites and sample patch management process <u>Vulnerability Management</u> Vulnerability management lifecycle understanding – Identify, Evaluate, Remediate, Report	1		2

								Types of vulnerabilities – Hardware, Network, Operating systems, Application, Human and Process related vulnerabilities Vulnerability Management process			
	3,4, 5	2,3, 4, 7	3	Practice Session: (a) Define one control statement each for access control, physical security and backup management (b) Explain one human vulnerability with example and how it can be exploited including remedial measures (c) Design IT asset register template with 5 sample rows populated with data Give examples for each category of classified information in an organization – do a combination of government organization and private organisation			4	ITIL Process overview – Incident Management, Problem Management, Change Management, Configuration Management, Release Management, Supplier Management, IT Security Management, Service level management, Capacity Management, Availability Management, Service continuity Management			3
			4	Security frameworks and Compliances			4	Cyber Security Governance:	1		2

				Introduction to standards/best practices/framework and its primary objective, ISO 27001, COBIT, PCI-DSS, Hi-Tech (HIPAA), NIST, IT Act 2000 (amendment in 2008), CERT-IN Guidelines. Regulatory requirements (a) RBI framework for banking (Cyber security framework, Gopalakrishna committee, UCB tiered framework) (b) SEBI framework for Securities market (c) Guidelines on Information and cyber security for insurers from IRDAI (d) TRAI requirements on security for telecom sector (e) GDPR				(a) Security organization, Responsibilities and authority, Management/Board responsibilities on cyber security, Resource allocation and cyber security budget management, Security Education, training and awareness, Cyber metrics, KRI/KPIs			
			5	**CIE 5 – Written and Practice Test**				Assessment Review and corrective action		3	

	3,4	2,3, 4,7	6	**Industrial class :** 1. An industry perspective of GRC, VM and Security frameworks Demo of a GRC tool				Weekly Assignment (Suggestive Student Activities) (a) Identify use case of how changes or configuration in IT systems impacts security configuration resulting in cyber risk exposure (b) Design a sample cyber security dashboard for reporting to top management (c) Give two KRI examples each for the following domains: a. Patch Management b. Anti-virus management c. Change Management			

References :

1) https://www.armosec.io/blog/kubernetes-security-frameworks-and-guidance - Security Frameworks table

2) https://www.cybersaint.io/blog/what-is-grc

3) https://www.ibm.com/cloud/learn/grc

4) https://unece.org/fileadmin/DAM/trade/Publications/WP6_ECE_TRADE_390.pdf

5) https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

6) https://www.nist.gov/

7) https://www.isaca.org/resources/cobit

8) https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf

9) https://www.coso.org/SitePages/Guidance-on-Enterprise-Risk-Management.aspx?web=1

10) https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

11) https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf

1) https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI129BB26DEA3F5C54198BF24774E1222E61A.PDF

14) https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html

15) https://www.sebi.gov.in/sebiweb/home/HomeAction.do?doListing=yes&sid=1&ssid=6&smid=0

16) https://www.aicofindia.com/AICEng/General_Documents/Notices%20And%20Tenders/IRDAI-GUIDELINES.pdf

17) https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4315&flag=1

18) https://www.rapid7.com/fundamentals/patch-management/

19) https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/

1)18. https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

21)https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/07.04.2017-Guidelines%20on%20Information%20and%20Cyber%20Security%20for%20insurers.pdf

https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

12	3,4, 5	2,3, 4	1	Peer review Project status review		4		DevOps and Security Challenges Understand the Core Principles and Patterns behind DevOps Recognize how DevOps works and identify keys to success	1		2
	3,4, 5	2,3, 4	2	Secure DevOps tools and workflows Conduct effective risk assessments and threat modeling in a rapidly changing environment Design and write automated security tests and checks in CI/CD Understand the strengths and weaknesses of different automated testing approaches in Continuous Delivery Inventory and patch your software dependencies Wire security scanning into Jenkins, Code Pipeline, and Azure DevOps workflows	1		3	Pre-Commit Security Controls Rapid Risk Assessment Git Hook Security Code Editor Extensions Branch Protections CodeOwners Peer Reviews Commit Security Controls Static Analysis Security Testing Component Analysis	1		2
	3,4, 5	2,3, 4	3	Secrets Management Managing secrets in CI / CD			4	Cloud Infrastructure as Code			3

				Azure Key Vault AWS SSM Parameter Store AWS Secrets Manager HashiCorp Vault				Introduction to Cloud Infrastructure as Code AWS Cloud Formation Terraform Deploying Cloud Infrastructure as Code security analysis			
	3,4, 5	2,3, 4	4	Configuration Management as Code Automating Configuration Management in CI / CD Using Ansible to Configure Virtual Machines Building Gold Images with Vagrant and Packer Certifying Gold Images with InSpec	1		3	Container Security Dockerfile and BuildKit Security Base Image Hardening with Hadolint and Conftest Container Image Security Scanning Container Images with Docker Scan and Trivy Container Registry Security Container Scanning with AWS ECR and Azure ACR Container Runtime Security Exercises Attacking the DevOps Toolchain Version Control Security Automating Static Analysis Protecting Secrets with Vault Infrastructure as Code Network Hardening Gold Image Creation Container Security Hardening	1		2

			5	**Developmental Assessment**				Assessment Review and corrective action			
			6	Industry Class :	2		3				
13			1	**Internship** **a) Secondary research on various industries and their operations to identify at least 3 companies along with the areas of work interest and develop an internship plan that clearly highlights expectations from the industry during the internship.** **b) Design and develop a cover letter for an internship request to all 3 identified companies and the resume to be submitted to potential companies.** **c) Prepare for an internship interview to highlight your interests, areas of study, career aspirations and personnel competence – including the areas of learning you expect to learn during internship.**				**Project** **a) Identification of the problem statement (from at least 3 known problems) the students would like to work as part of the project – either as provided by faculty or as identified by the student. Document the impact the project will have from a technical, social and business perspective.** **b) Design and develop the project solution or methodology to be used to solve at least one of the problems identified.** **c) Prepare a project plan that will include a schedule, WBS, Budget and known risks along with strategies to mitigate them to ensure the project achieves the desired outcome.**			

****Note:** Saturday session from 9 AM -2 PM

CIE and SEE Assessment Methodologies

CIE Assessment	Assessment Mode	Duration In hours	Max Marks
Week 3	CIE 1– Written and practice test	4	30
Week 5	CIE 2– Written and practice test	4	30
Week 7	CIE 3– Written and practice test	4	30
Week 9	CIE 4– Written and practice test	4	30
Week 11	CIE 5– Written and practice test	4	30
	On line Course work (Minimum 10 hours online course with certification from (SWAYAM/NPTEL/Infosys Springboard)		40
	Profile building for Internship / Submission of Synopsys for project work		20
Portfolio evaluation (Based on industrial assignments and weekly developmental assessment) *			30
TOTAL CIE MARKS (A)			**240**
SEE 1 - Theory exam (QP from BTE) Conducted for 100 marks 3 hrs duration reduced to 60 marks		**3**	**60**
SEE 2 – Practical		**3**	**100**
TOTAL SEE MARKS (B)			**160**
TOTAL MARKS (A+B)			**400**

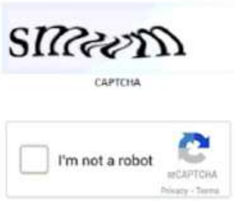
* The industrial assignment shall be based on peer-to-peer assessment for a total of 10 marks (on a scale of 1 to 10) and in the event of a group assignment the marks awarded will be the same for the entire group, the developmental assessment will be for a total of 20 marks and based on MCQ/case study/demonstration and such other assignment methods

Assessment framework for CIE

Note : Theory to be conducted for 1 hour and practice for 3 hours, total duration of exam – 4 hours

Programme	**Computer Science & Engineering**	**Semester**	**V**
Course	**Cyber Security**	**Max Marks**	**30**
Course Code	**20CS54I**	**Duration**	**4 hours**
Name of the course coordinator			

Note: Answer one full question from each section.

Qn.No	Question	CL L3/L4	CO	PO	Marks
	Section-1 (Theory) – 10 marks				
1.a)	Why do see this kind of "Captcha" in web applications ? What difference does it make to any  web based application ?	L4	1		6
b)	Your creating new password for your online banking, how will you strengthen your password elaborate ?	L4	1		4
2.a)	Let p = 191 and q = 2. Alice picks x = 42 and B picks y = 33. Compute the shared secret between Alice and Bob using Diffie-Hellman key exchange protocol.	L4	1		5
b)	Given an implementation of RSA algorithm that uses primes p = 5 and q = 11, if the encryption key is 27, what is the decryption key?	L4	1		5
	Section-2 (Practical) - 20 marks				
3).a	You've just been issued with a new laptop at your organization and are getting ready to set it up. What steps would you take to secure it before use?	L4	1		10

<table>
<tr>
<td></td>
<td><b>Scheme of evaluation</b>
<table>
<tr><th>Sl. No</th><th>Description</th><th>Marks</th></tr>
<tr><td>1</td><td>Setting up password</td><td>5</td></tr>
<tr><td>2</td><td>Installing antivirus and fire wall</td><td>10</td></tr>
<tr><td>3</td><td>Firewall Windows/Linux settings</td><td>5</td></tr>
<tr><td colspan="2">Total</td><td>20</td></tr>
</table>
</td>
<td></td><td></td><td></td><td></td>
</tr>
<tr>
<td>b</td>
<td>Design a simple crypto system (including key generation, encryption, decryption, digital signature or hash function) using any tool

<b>Scheme of evaluation</b>
<table>
<tr><th>Sl. No</th><th>Description</th><th>Marks</th></tr>
<tr><td>1</td><td>Designing crypto system</td><td>5</td></tr>
<tr><td>2</td><td>Key generation</td><td>5</td></tr>
<tr><td>3</td><td>Encryption/Decryption</td><td>5</td></tr>
<tr><td>4</td><td>digital signature or hash function</td><td>5</td></tr>
<tr><td colspan="2">Total</td><td>20</td></tr>
</table>
</td>
<td></td><td></td><td></td><td></td>
</tr>
</table>

Note : Theory questions shall be aligned to practical questions

Assessment framework for SEE (Theory) – 100 Marks / 3 hours (Reduced to 60 marks)

Programme:	**Computer Science & Engineering**	**Semester: V**
Course:	**Cyber Security**	**Max Marks: 100**
Course Code:	**20CS54I**	**Duration: 3 Hrs**

Instruction to the Candidate:
Answer one full question from each section.

Qn.No	Question	CL	CO	Marks
	Section-1			
1.a)	Which is the security protocol applied at layer 3 of the OSI stack? What are its benefits	L3/L4	1	10
b)	What is the need of defence in depth for a network ?	L3/L4		10
2.a)	How do you apply Microsoft Secure SDLC in each stage of software development ?	L3/L4		12
b)	Your creating new password for your online banking, how will you strengthen your password elaborate ?	L3/L4		8
	Section-2			
3.a)	Let p = 191 and q = 2. Alice picks x = 42 and B picks y = 33. Compute the shared secret between Alice and Bob using Diffie-Hellman key exchange protocol.	L3/L4	2	14
b)	Find Euler totient function: $\varphi(255)$, $\varphi(256)$	L3/L4		6
4.a)	Given an implementation of RSA algorithm that uses primes p = 5 and q = 11, if the encryption key is 27, what is the decryption key?	L3/L4		12
b)	What is the final digit and two final digits of 3^{10000}?	L3/L4		8
	Section- 3			
5.a)	Describe Stages and life cycle of incident management	L3/L4	3	12
b)	What is the need of Dynamic File analysis ?	L3/L4		8
6.a)	Create a Threat Model for a social media Web Application at Design Time	L3/L4		10

b)	Describe shared responsibility model in cloud	L3/L4		10
	Section-4			
7.a)	How do you find vulnerability in your cloud based web application ? what are the common vulnerabilities ?	L4	4	12
b)	Illustrate setting up multi factor authentication on any public cloud system	L3		8
8.a)	Highlight deprecated unsafe functions in common programming languages	L4		10
b)	What is the need of static code analysis, Static Code Analysis Tools – Explain with examples	L4		10
	Section-5			
9.a)	Illustrate lifecycles of security incident management	L3	5	8
b)	Design a sample cyber security dashboard for reporting to top management	L4		12
10.a)	Identify use case of how changes or configuration in IT systems impacts security configuration resulting in cyber risk exposure	L4		12
b)	Give two KRI examples each for the following domains: a. Patch Management b. Anti-virus management	L4		8

Assessment framework for SEE 2 (Practice)

Problem Statement : Conduct Penetration testing on any web site/web application and report the vulnerabilities	
Scheme of Evaluation	
1) Installing ZAP	20
2) Running an automated scan	20
3) Exploring the application manually 1. Explore pages protected by login 2. Exploring web application over a defined sequence	30
4) Prepare a vulnerability report	20

5) Viva-voce (about the attack on discovered vulnerability and possible solutions)	10
Total	100

Note: Examiner to prepare/identify the web site/application to be tested and the vulnerabilities present in the web site/web application before exam

Equipment/software list with Specification for a batch of 20 students

Sl. No.	Particulars	Specification	Quantity
12.	Computers	Intel i5, 4GB RAM, 500GB SSD	**20**
13.	Cloud – AWS/AZURE/GCP or any similar public cloud environment		**20**
14.	Broadband connection	Atleast 50MBPS	**1**