CURRICULUM FOR

POST GRADUATE DIPLOMA COURSE IN CYBER SECURITY

(Duration: One Year)
Semester System

FOR THE STATE OF UTTAR PRADESH

ज्ञानं प्रकाशयति तत्परम

Prepared by:
Institute of Research Development & Training, Kanpur

APPROVED IN CDC MEETING OF BOARD OF TECHNICAL EDUCATION,U.P,LUCKNOW DATED:26-05-2022

CONTENTS

Sr. No	Particulars	Page No.
1.	Salient Features of the Diploma Programme	5
2.	Employment Opportunities	6
3.	Learning Outcomes of the Programme	7-8
4.	Deriving Curriculum Areas from Learning Outcomes of the Programme	9-11
5.	Abstract of Curriculum Areas	12
6.	Horizontal and Vertical Organization of the Subjects	13-15
7.	Study and Evaluation Scheme	16-17
8.	Guidelines (for Assessment of Student Cantered Activities and Internal Assessment)	18
9.	Detailed Contents of various Subjects	19-44

FIRST SEMESTER

1.1	Fundamentals of Cyber Security	19-21
1.2	Networking Concepts & Security	22-24
1.3	Operating System Security & Forensics	25-27
1.4	Fundamentals of Web Application and Security	28-30
1.5	Project-I	31

SECOND SEMESTER

2.1	Cryptography	32-34
2.2	Cyber Crime, Laws & Forensic Investigation	35-37
2.3	Mobile Concepts & Security	38-40
2.4	Seminar: Paper Presentation	41-42
2.5	Project-II	43-45

10.	Resource Requirement	46-47
11.	Evaluation Strategy	48-50
12.	Recommendations for Effective Implementation of Curriculum	51-53
13.	List of Participants	54

PREFACE

An important issue generally debated amongst the planners and academician's world over is how technical education can contribute to sustainable development of the societies struggling hard to come in the same bracket as that of the developed nations. The rapid industrialization and globalization have created an environment for free flow of information and technology through fast and efficient means. This has led to shrinking of the world, bringing people from different culture and environment together and giving rise to the concept of world turning into a global village. In India, a shift has taken place from the forgettable years of closed economy to knowledge based and open economy in the last few decades. In order to cope with the challenges of handling new technologies, materials and methods, we have to develop human resources having appropriate professional knowledge, skills and attitude. Technical education system is one of the significant components of the human resource development and has grown phenomenally during all these years. Now it is time to consolidate and infuse quality aspect through developing human resources, in the delivery system. Polytechnics play an important role in meeting the requirements of trained technical manpower for industries and field organizations. The initiatives being taken by the Department of Technical Education, UP to run new age diploma programmes as per the needs of the industry and making them NSQF compliant, are laudable.

In order to meet the requirements of future technical manpower, we will have to revamp our existing technical education system and one of the most important requirements is to develop outcome-based curricula of diploma programmes. The curricula for diploma programmes have been developed & revised by adopting time-tested and nationally acclaimed scientific method, laying emphasis on the identification of learning outcomes of diploma programme.

The real success of the diploma programme depends upon its effective implementation. However best the curriculum document is designed, if that is not implemented properly, the output will not be as expected. In addition to acquisition of appropriate physical resources, the availability of motivated, competent and qualified faculty is essential for effective implementation of the curricula.

It is expected from the polytechnics to carry out job market research on a continuous basis to identify the new skill requirements, reduce or remove outdated and redundant courses, develop innovative methods of course offering and thereby infuse the much-needed dynamism in the system.

Manoj Kumar

Director

Institute of Research Development & Training

Kanpur, U.P.

ACKNOWLEDGEMENTS

We gratefully acknowledge the guidance and contribution received from the following persons:

- Sh. Subhash Chand Sharma, IAS, Principal Secretary, Technical Education Department, U.P. Govt.
- Sh. Sunil Kumar Chaudhary, IAS, Special Secretary, Technical Education Department, U.P. Govt.
- Sh. Manoj Kumar, Director, Technical Education, U.P. and I.R.D.T., Kanpur, for taking keen interest in the development of this curriculum.
- Secretary, Board of Technical Education, UP for initiating this project of development of curriculum.
- All the participants from industry/field organizations, engineering colleges, polytechnics and other technical institutions for their professional inputs during curriculum workshops.
- All Faculty/Subject Experts from Uttar Pradesh Government Polytechnics.

Coordinator
Institute of Research Development & Training,
Kanpur, U.P.

1. SALIENT FEATURES OF POST GRADUATE DIPLOMA IN CYBER SECURITY

1)	Name of the Programme	:	P.G. Diploma in Cyber Security
2)	Duration of the Programme	:	One year (Two Semesters)
3)	Entry Qualification	:	B.Tech/PGDCA/B.Sc.-IT/B.Sc-CS/BCA/Graduate with O Level certificate/ computer background or as Prescribed by State Board of Technical Education, UP
4)	Intake	:	75 (or as prescribed by the Board)
5)	Pattern of the Programme	:	Semester Pattern
6)	NSQF Level	:	Level - 8
7)	Ratio between theory and Practice	:	1: 2 (Approx.)

8) **Industrial Training**

Minimum Four weeks of industrial training is included after Ist semester during semester break vacation. Total marks allotted to industrial training will be 50.

9) Student Centered Activities

A provision of 3-6 hrs. per week has been made for organizing Student Centred Activities for overall personality development of students. Such activities will comprise of co–curricular activities such as expert lectures, self-study, games, hobby classes like photography, painting, singing etc. seminars, declamation contests, educational field visits, NCC, NSS and other cultural activities, disaster management and environmental safety etc.

10) Project work

A project work in the 1st & 2nd semester has been included in the curriculum to enable the students to get familiar with the practices and procedures being followed in the industries and provide an opportunity to work on some live projects in the industry.

2. EMPLOYMENT OPPORTUNITIES FOR PG DIPLOMA HOLDERS IN CYBER SECURITY

PG Diploma holders in Cyber Security can find employment in following sectors:

- Service Division (IT enabled services, maintenance service and installation of computer services)
- Software Development and Testing Industries
- Web Development and Testing Industries
- Mobile Applications Development and Testing Industries
- Lab. Assistant/Technician
- Hospitals/Healthcare/Institutions/Schools
- Cloud Services Support Engineer
- Telecommunication Sector
- Teaching Organizations (Polytechnics, Vocational Institutions etc)
- Networking (LAN, WAN etc)
- Defence Services/Police Services/Cyber Services/Forensic Services

3. LEARNING OUTCOMES OF PG DIPLOMA HOLDERS IN CYBER SECURITY

After undergoing this programme, students will be able to:

Sr No.	Learning Outcomes
1.	Understand cyber security concepts.
2.	Learn different types of cyber-attacks.
3.	Categorise the types of cyber security.
4.	Learn the general procedures adopted for cyber-attacks.
5.	Understand the fundamentals and security concepts of networking.
6.	Learn and implement the Virtual private Networks.
7.	Learn the strategy behind different types of network attacks & their prevention by using open source tools.
8.	Understand the types of wireless attacks & their prevention by using open source tools.
9.	Understand the fundamentals of operating system.
10.	Implement the process of securing an OS.
11.	Understand the principles of trusted systems, Information flow integrity and Harding OS.
12.	Understand the Kali Linux OS, its administration & security.
13.	Learn the operating system forensics
14.	Web security aims to prevent such attacks by denying unauthorized access, usage, destruction/disruption, or modification.
15.	This course provides the knowledge and skills Testers need to detect security vulnerabilities in web applications.
16.	Learn web application penetration testing and ethical hacking through current course content, hands-on labs, and an immersive capture-the-flag challenge.

17.	Web application penetration testing is comprised of four main steps including information gathering, research and exploitation
18.	Understand the concepts of cryptography.
19.	Understand different classical ciphers used for cryptography.
20.	Differentiate between Symmetric and Asymmetric Key Cryptographic Techniques.
21.	Understand different Public Key cryptosystem algorithms.
22.	Understand the concept and usage of Cryptocurrency.
23.	Understand different Authentication Techniques & Protocols.
24.	Understand the types of cyber-crimes, issues and security policies.
25.	Understand the Cyber Laws & IT Act 2000 framework in India.
26.	Understand the categorization of various offences & penalties.
27.	Understand the steps of recording forensic investigation.
28.	Understand the fundamentals of mobile system and its security.
29.	Understand the technologies used in a mobile based approach.
30.	Understand the types & working of various mobile networks.
31.	Know the tools & various technologies used for mobile management and security.
32.	Understand various types of attacks by testing different mobile OS.

4. DERIVING CURRICULUM AREAS FROM LEARNING OUTCOMES OF THE PROGRAMME

The following curriculum area subjects have been derived from learning outcomes:

Sr No.	**Learning Outcomes**	Curriculum area subjects
1.	Understand cyber security concepts	Fundamentals of Cyber Security
2.	Learn different types of cyber-attacks.	Fundamentals of Cyber Security
3.	Categorise the types of cyber security.	Fundamentals of Cyber Security
4.	Learn the general procedures adopted for cyber-attacks.	Fundamentals of Cyber Security
5.	Understand the fundamentals and security concepts of networking.	Networking Concepts & Security
6.	Learn and implement the Virtual private Networks.	Networking Concepts & Security
7.	Learn the strategy behind different types of network attacks & their prevention by using open source tools.	Networking Concepts & Security, Fundamentals of Cyber Security
8.	Understand the types of wireless attacks & their prevention by using open source tools.	Networking Concepts & Security
9.	Understand the fundamentals of operating system.	Operating System Security & Forensics
10.	Implement the process of securing an OS.	Operating System Security & Forensics
11.	Understand the principles of trusted systems, Information flow integrity and Harding OS.	Operating System Security & Forensics
12.	Understand the Kali Linux OS, its administration & security.	Operating System Security & Forensics

13.	Learn the operating system forensics	Operating System Security & Forensics
14.	Web security aims to prevent such attacks by denying unauthorized access, usage, destruction/disruption, or modification.	Fundamentals of Web Application and Security
15.	This course provides the knowledge and skills Testers need to detect security vulnerabilities in web applications.	Fundamentals of Web Application and Security
16.	Learn web application penetration testing and ethical hacking through current course content, hands-on labs, and an immersive capture-the-flag challenge.	Fundamentals of Web Application and Security
17.	Web application penetration testing is comprised of four main steps including information gathering, research and exploitation	Fundamentals of Web Application and Security
18.	Understand the concepts of cryptography.	Cryptography
19.	Understand different classical ciphers used for cryptography.	Cryptography
20.	Differentiate between Symmetric and Asymmetric Key Cryptographic Techniques.	Cryptography
21.	Understand different Public Key cryptosystem algorithms.	Cryptography
22.	Understand the concept and usage of Cryptocurrency.	Cryptography
23.	Understand different Authentication Techniques & Protocols.	Cryptography
24.	Understand the types of cyber-crimes, issues and security policies.	Cyber Crime, Laws & Forensic Investigation
25.	Understand the Cyber Laws & IT Act 2000 framework in India.	Cyber Crime, Laws & Forensic Investigation
26.	Understand the categorization of various offences & penalties.	Cyber Crime, Laws & Forensic Investigation

27.	Understand the steps of recording forensic investigation.	Cyber Crime, Laws & Forensic Investigation
28.	Understand the fundamentals of mobile system and its security.	Mobile Concepts & Security
29.	Understand the technologies used in a mobile based approach.	Mobile Concepts & Security
30.	Understand the types & working of various mobile networks.	Mobile Concepts & Security
31.	Know the tools & various technologies used for mobile management and security.	Mobile Concepts & Security
32.	Understand various types of attacks by testing different mobile OS.	Mobile Concepts & Security

5. ABSTRACT OF CURRICULUM AREAS

a) Basic Courses in Engineering/Technology

- Fundamentals of Cyber Security
- Networking Concepts & Security
- Fundamentals of Web Application and Security
- Cryptography

b) Applied Courses in Engineering/Technology

- Operating System Security & Forensics
- Cyber Crime, Laws & Forensic Investigation
- Mobile Concepts & Security

c) Industrial Training/Project

- Project /Internship

6. HORIZONTAL AND VERTICAL ORGANISATION OF THE SUBJECTS

Sr. No.	Subjects	Distribution in Periods per week in Various Semesters	
		I	II
1.	Fundamentals of Cyber Security	08	-
2.	Networking Concepts & Security	10	-
3.	Operating System Security & Forensics	12	-
4.	Fundamentals of Web Application and Security	10	-
5.	Cryptography	-	12
6.	Cyber Crime, Laws & Forensic Investigation	-	06
7.	Mobile Concepts & Security	-	10
8.	Seminar: Paper Presentation	-	02
9.	Project	04	06
10.	Student Centred Activities	02	02
Total		**46**	**38**

NEED ANALYSIS

Over the past year, we’ve witnessed all the hype surrounding cyber security finally transformed into a frightening new reality, where corporate and government organizations seem helpless to stop cyber incursions. Cyber-attacks have become nonstop headline news. The transformation from perceived threat to actual headlines has occurred for the following reasons:

Hacking, cracking and other forms of cyber mischief have reached a level of sophistication equalling (and in many cases surpassing) the capability of most organizations to defend against.

Those practicing cyber-attacks in 2022 are hardened professionals with more years of actual technical security experience than the average IT worker employed to defend against them. The days of the amateur hacking enthusiast are largely gone. Cyber-attacks today are conducted by nation states, terrorist groups and crime syndicates. It is no longer a hobby; it is a profession with very high stakes involved.

As people rely more heavily on technology to help manage their daily lives, the threat of cybercrime continues to escalate.

According to a recent study, there is shortage of cyber security professionals worldwide. Traditional IT professionals may not be fully trained in information security tactics, and some organizations may not be willing or able to spend a significant amount of money on companywide cyber security awareness training.

One way to fight cybercrime is to effectively educate the students through cyber security courses. Cyber-attacks pose a threat to everyone, not just companies. It’s important to educate users about cyber security in order to help them protect their personal information from cyber thieves.

JOB POTENTIAL/JOB OPPORTUNITIES

Training and awareness are important for educating the students, but cyber security professionals are vital in today's business world. They help develop new ways to combat cyber threats, and are the main line of defence against spamming, phishing, malware, viruses and other information security threats.

As cyber-attacks have increased, so has the demand for professionals who are trained to stop such attacks.

According to a study, the job outlook for cyber security professionals is strong. For example, employment of Information Security Analysts is projected to increase by 33% between 2020 to 2030, much faster than the national average for all occupations (www.bls.gov). India is expected to have over 1.5 million unfulfilled job vacancies in cybersecurity by 2025.

COURSE OBJECTIVE

The participants of this course will be able to:

1. Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.

2. Understand key terms and concepts in cyber law, intellectual property and cybercrimes, trademarks and domain theft.

3. Determine computer technologies, digital evidence collection, and evidentiary reporting in forensic acquisition.

4. Incorporate approaches to secure networks, firewalls, intrusion detection systems, and intrusion prevention systems.

5. Examine secure software construction practices.

6. Understand principles of web security.

7. Incorporate approaches for incident analysis and response.

8. Incorporate approaches for risk management and best practices.

STUDY & EVALUATION SCHEME FOR ONE YEAR PG DIPLOMA IN CYBER SECURITY

Semester System

(Effective from session 2022-23)

FIRST SEMESTER

Sr. No.	SUBJECTS	STUDY SCHEME Periods/Week			Credits	MARKS IN EVALUATION SCHEME								Total Marks of Internal & External
						INTERNAL ASSESSMENT			EXTERNAL ASSESSMENT					
		L	T	P		*Th*	Pr	Tot	Th	Hrs	Pr	Hrs	Tot	
1.1	Fundamentals of Cyber Security	4	-	4	5	20	30	50	50	2 ½	50	3	100	150
1.2	Networking Concepts & Security	6	-	4	6	20	30	50	50	2 ½	50	3	100	150
1.3	Operating System Security & Forensics	6	-	6	6	20	30	50	50	2 ½	50	3	100	150
1.4	Fundamentals of Web Application and Security	6	-	4	6	20	30	50	50	2 ½	50	3	100	150
1.5	Project-I	-	-	4	2	-	20	20	-	2 ½	50	3	50	70
#Student Centred Activities		-	-	2	1	-	30	30	-	-	-	-	-	30
Total		22	-	24	26	80	170	250	200	-	250	-	450	700

# Student Centered Activities will comprise of co-curricular activities like extension lectures, games, hobby clubs e.g. photography etc., seminars, declamation contests, educational field visits, N.C.C., NSS, Cultural Activities, self study etc.

Industrial Training: Minimum Four weeks of industrial training is included after Ist semester during semester break vacation.

SECOND SEMESTER

Sr. No.	SUBJECTS	STUDY SCHEME Periods/Week			Credits	MARKS IN EVALUATION SCHEME								Total Marks of Internal & External
						INTERNAL ASSESSMENT			EXTERNAL ASSESSMENT					
		L	T	P		*Th*	Pr	Tot	Th	Hrs	Pr	Hrs	Tot	
2.1	Cryptography	6	-	6	6	20	30	50	50	2 ½	50	3	100	150
2.2	Cyber Crime, Laws & Forensic Investigation	6	-	-	6	20	-	20	50	2 ½	-	-	50	70
2.3	Mobile Concepts & Security	4	-	6	6	20	30	50	50	2 ½	50	3	100	150
2.4	Seminar: Paper Presentation	-	-	2	2	-	50	50	-	-	50	-	50	100
2.5	PROJECT													
	I: Industrial Training	-	-	-	2	-	50	50	-	-	-	-	-	
	II: Project-II	-	-	6	4	-	50	50	-	-	100	4	100	200
#Student Centred Activities		-	-	2	1	-	30	30	-	-	-	-	-	30
Total		**16**	**-**	**22**	**27**	**60**	**240**	**300**	**150**	**-**	**250**	**-**	**400**	**700**

- Student Centered Activities will comprise of co-curricular activities like extension lectures, games, hobby clubs e.g. photography etc., seminars, declamation contests, educational field visits, N.C.C., NSS, Cultural Activities, self study etc.
- Industrial Training: Minimum Four weeks of industrial training is included after Ist semester during semester break vacation.

8. GUIDELINES FOR ASSESSMENT OF STUDENT-CENTRED ACTIVITIES (SCA)

It was discussed and decided that the maximum marks for SCA should be 30 as it involves a lot of subjectivity in the evaluation. The marks may be distributed as follows:

i. 10 Marks for general behaviour and discipline
(By HODs in consultation with all the teachers of the department)

ii. 5 Marks for attendance as per following:
(By HODs in consultation with all the teachers of the department)

a)	75 - 80%	2 Marks
b)	80 - 85%	4 Marks
c)	Above 85%	5 Marks

iii. 15 Marks maximum for Sports/NCC/Cultural/Co-curricular/ NSS activities as per following:
(By In-charge Sports/NCC/Cultural/Co-curricular/NSS)

a)	15	-	State/National Level participation
b)	10	-	Participation in two of above activities
c)	5	-	Inter-Polytechnic level participation

Note: There should be no marks for attendance in the internal sessional of different subjects.

1.1 Fundamentals of Cyber Security

L	T	P
4	0	4

RATIONALE

This course will be responsible for establishing a comprehensive understanding in the field of cyber security. With a view that incumbents in this diploma course are from varied disciplines, after studying this paper all the students would be able to come at par and move together as they must go deeper into hard-core cyber security topics during the course duration.

LEARNING OUTCOMES

After undergoing the subject, the students will be able to:

- Understand cyber security concepts.
- Learn different types of cyber-attacks.
- Categorise the types of cyber security.
- Learn the general procedures adopted for cyber-attacks.

DETAILED CONTENTS

Unit 1. Cyber Security (10 Period)

Introduction to cyber security, information security, network security, application and system security, Threats to Information Systems, Information Assurance, Security Risk Analysis, Security Principles or Security Goals (CIA Principle), Security Services, Security Mechanism, Security Technique: Cryptography & Steganography, Active & Passive Attacks. Hardware & network Basics, Basic terminologies in cyber security: Cloud, Software, Domain, VPN, IP Address, Exploit, Breach, Firewall, Malware, Virus, Ransomware, Trojan Horse, Worm, Bot/Botnet, Spyware, Rootkit, DDOS, Phishing/Spear Phishing, Encryption. Security Threats - Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack

Unit 2. System & Application security (06 Period)

System Hacking Concepts: Gaining access, cracking passwords, vulnerability exploitation, escalating privileges, hiding files, clearing logs,
Data Security Considerations: Backups, Archival Storage and Disposal of Data
Security Technologies: Firewall and VPNs, Intrusion Detection, Access Control Security

Unit 3. Web Security (10 Period)

Introduction- A web security forensic lesson, Introduction to different web attacks. Overview of N-tier web applications, Web Hacking Basics HTTP & HTTPS URL, Web under the Cover, Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions

Unit 4. Cloud Security (15 Period)

Introduction to Cloud Computing, migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm.
Cluster: Admin Server & Managed Server
Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS) Virtual machines provisioning and Migration services, On the Management of Virtual machines for Cloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing, Aneka, Comet Cloud, T-Systems', Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments.

Unit-5. General Procedure adopted for Cyber Attacks: (15 Period)

Reconnaissance: Foot printing concepts and methodology, foot printing using -search engines, web services, social networking sites, website, email, whois, DNS, network, foot printing by social engineering, foot printing tools, foot printing counter measures.
Scanning: concept, host discovery, OS discovery, scanning beyond IDS and Firewall, Drawing network diagram.
Enumeration: Concepts and Techniques, NetBIOS Enumeration.

List of Practical's

- Recovering the content of a virus infected storage media device.
- Password cracking using open-source tools.
- Learning different type of attacks.
- Study of firewall and implementation of protection mechanism.
- Service Development & usage over cloud using open source.
- Managing cloud computing resources
- Detecting Trojan Attacks using open-source tools.
- Implementing Foot printing using open-source tools.
- Implementing Fingerprinting using open-source tools.
- Implementing Poisoning & Exploitation using open-source tools.

INSTRUCTIONAL STRATEGY

The content of this course is to be taught on conceptual basis with real world examples. Since this subject is practice oriented, the teacher should demonstrate the capabilities of websites/Webpages to students while doing practical exercises for information security. The students should be made familiar with preventive measures for information and computer security.

MEANS OF ASSESSMENT

1. Assignments and quiz/class tests, mid-term and end-term written tests
2. Practical work, exercises and viva-voce
3. Software installation, operation and viva-voce

Reference Books:

- Security Analysis and Portfolio Management by Donald E. Fischer
- Professional Pen Testing for Web Applications by Andres Andreu
- Foundations of Security: What Every Programmer Needs to Know by by Christoph Kern (Author), Anita Kesavan (Author), Neil Daswani
- Cloud Computing by M N Rao, PHI Publication, 1st edition.
- Cloud Computing by Saurabh Kumar, Wiley Publication
- Cloud Computing Bible, Wiley Publication
- Social Media Security: Leveraging Social Networking While Mitigating Risk by Michael Cross
- Securing the Clicks Network Security in the Age of Social Media by by Gary Bahadur

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://nptel.ac.in/
4. https://cloud.google.com/docs/get-started

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	10	20
2	06	10
3	10	20
4	15	25
5	15	25
Total	**56**	**100**

1.2 Networking Concepts & Security

L	T	P
6	0	4

RATIONALE

This course focuses on teaching students about the fundamentals and distinctions of network building along with setup of present-day networks in complex environments. The networks today are vulnerable to various attacks and this paper aims at acquainting students with the techniques used by hackers for network attacks and also the techniques adopted in order to guard the entire infrastructure against various attacks.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the fundamentals and security concepts of networking.
- Learn and implement the Virtual private Networks.
- Learn the strategy behind different types of network attacks & their prevention by using open source tools.
- Understand the types of wireless attacks & their prevention by using open source tools.

DETAILED CONTENTS

Unit I: Introduction to Network Security (14 Periods)
Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP/IP Model, TCP Vs. UDP, Routers, Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based) and setup.

Unit II: Virtual Private Networks (10 Periods)
VPN and its types –Tunnelling Protocols – Tunnel and Transport Mode –Authentication Header Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE 1, II – Generic Routing Encapsulation (GRE). Implementation of VPNs.

Unit III: Network Attacks Part 1 (20 Periods)
Sniffing concepts, Sniffing Techniques: MAC Attack, DHCP attack, ARP poisoning, Spoofing, DNS poisoning. Wireshark, packet analysis, display and capture filters, Ettercap, sniffing counter measures, sniffing protection tools.

Denial of service (DOS)/Distributed Denial of service (DDOS): Concepts, DOS/DDOS Technique, Botnets, DDOS, DOS/DDOS attacking tools, DOS/DDOS counter Measures, DOS/DDOS protection tools.
Vulnerability scanning tools: Concepts, Scanning Techniques, Tools: Nessus, OpenVAS, Sparta, Nexpose, Nmap. Network Scanning Report Generation, Striping, Router attacks, VPN pentesting, VOIP pentesting, Enumeration techniques: SMTP, SNMP, IPsec, VOIP, RPC, Telnet, FTP, TFTP, SMP, IPV6 and BGP.

Unit IV: Network Attacks Part 2 **(20 Periods)**
Network Exploitation OS Detection in network, Scanning: nmap, open ports, filtered ports, service detection, metasploit framework, interface of metasploit framework, network vulnerability assessment, evade anti viruses and firewalls, metasploit scripting, exploits, vulnerabilities, payloads, custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploits delivery, burp-suite, End Point Security.

Unit V: Wireless Attacks **(20 Periods)**
Wireless concept, wireless encryption, wireless threats, wireless hacking methodology, wireless hacking and security tools, Bluetooth hacking, countermeasures to wireless threats, Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentications, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

List of Practical's

- Brute force attack using open-source tools.
- Identifying network attacks using Nmap, Metasploit.
- Selecting a Capture Interface and creating the first pcap file using Wireshark.
- Using Capture filters in Wireshark.
- Finding a Text String in a Trace File using Wireshark.
- Understanding Packet Loss and Recovery process.
- Identifying DOS & DDOS Attack.
- VPN & VOIP pentesting using open-source tools.
- Demonstration of IDS using snort or any other open-source tool.
- Demonstration of IPS using snort or any other open-source tool.

INSTRUCTONAL STRATEGY

The content of this course is to be taught on conceptual basis with real world examples. Since this subject is practice oriented, the teacher should demonstrate the capabilities of websites/Webpages to students while doing practical exercises for information security. The students should be made familiar with preventive measures for information and computer security.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Practical work, exercises and viva-voce

– Software installation, operation and viva-voce

Reference Books:

- Computer Networks by Tanenbaum; Prentice Hall of India, New Delhi
- Data Communications and Networking by Forouzan, (Edition 2nd and 4th); Tata McGraw Hill Education Pvt Ltd , New Delhi
- Data and Computer Communication by William Stallings; Pearson Education, New Delhi
- Information Security: The Complete Reference, Second Edition by Mark Rhodes-Ousley
- Principles of Information Security by Whitman
- Cryptography and Network Security: Principles and Practice by William Stallings
- Cryptography Theory & Practice by Douglas Stinson
- Understanding Cryptography: A Textbook For Students And Practitioners by Paar
- Information Security by Pankaj Sharma
- Charles P. Pfleeger, Shari Lawerance Pfleeger, "Analysing Computer Security "
- V.K. Pachghare, "Cryptography and information Security",

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://wiresharklabs.com
4. https://www.snort.org/

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	**Time Allotted (Periods)**	**Marks Allotted (%)**
1	14	20
2	10	5
3	20	25
4	20	25
5	20	25
Total	**84**	**100**

1.3 Operating System Security & Forensics

L	T	P
6	0	6

RATIONALE

This paper introduces students about threats and vulnerabilities in an operating system. It also makes them able to understand the installation and features of Kali Linux and how to establish the security in various operating systems. It focuses on the study of different tools & techniques used for OS Security along with protection systems, Information flow and OS Forensics.

LEARNING OUTCOMES

- After undergoing this course, the students will be able to:
- Understand the fundamentals of operating system.
- Implement the process of securing an OS.
- Understand the principles of trusted systems, Information flow integrity and Harding OS.
- Understand the Kali Linux OS, its administration & security.
- Learn the operating system forensics

DETAILED CONTENTS

Unit I: File System & Data Recovery (12 Periods)

File System Concept, File Structure, Attributes of a file, File Access method, Directory Structure, aspects of file systems, Types of file systems, File systems & operating systems, Data Backup & Recovery Solutions.

Unit II: Linux OS: Kali Linux (14 Periods)

Installation of Kali Linux, boot process, Basic Linux commands, Configuring the GRUB boot loader, Disk partition, Managing Kali Linux Services, Searching, Installing, and Removing Tools, Bash Scripting, Piping & Redirection, File and command monitoring, Network related commands.

Unit III: Linux OS Administration and Security (24 Periods)

Repository configuration, User administration of Linux, Network Configuring, Load balancing, SSH, VNC, Network Authentication, Perform System Management, Package management, configuring the Apache web server, SE LINUX, Basic Service Security, Log Management and NTP, BIND and DNS Security, Network Authentication: RPC, NIS and Kerberos, LDAP, LDAP Enumeration Technique, Apache security (SSL), Automate Task Using Bash Script, Security patches, IP Tables.

Unit IV: OS Security **(14 Periods)**

Introduction: Secure OS, Security Goals, OS Security Vulnerabilities, updates and patches, OS integrity checks, Anti-virus software, Design of secure OS and OS hardening, configuring the OS for security, Trusted OS, Threat Model, OS authentication mechanisms, Verifiable security goals: Information flow, information flow integrity model

Unit V: OS Forensics **(20 Periods)**

Types of digital media, booting process, types of information: volatile & non-volatile information, memory analysis, registry analysis, cache, cookie & history analysis in web browser, MD5 calculation for checking integrity of files, recycle bin/trash file analysis, prefetch files, file signature analysis, executable file analysis, Event log analysis.

List of Practical's

- ➢ Identifying the file system of an operating system
- ➢ Step by step Implementation of OS Hardening.
- ➢ Working with Information Gathering tools in Kali Linux: NMAP & ZENMAP
- ➢ Identifying vulnerabilities of an operating system
- ➢ Working with Vulnerability Analysis Tools in Kali Linux
- ➢ Working with Exploitation Tools in Kali Linux
- ➢ Working with Forensics Tools in Kali Linux
- ➢ Working with password cracking tools in kali Linux
- ➢ Use of keyloggers & anti keyloggers
- ➢ Implementation of IP tables in Linux

INSTRUCTONAL STRATEGY

This subject is both theory and practical oriented. Therefore, stress must be given on practical's along with theory. Concepts of O.S. must be taught practically.

MEANS OF ASSESSMENT

– Assignments and quiz/class tests, mid-term and end-term written tests
– Actual laboratory and practical work, exercises and viva-voce
– Software installation, operation, development and viva-voce

Reference Books:

- Operating System Concepts (2012) by Silber Schatz, Galvin and Gagne.
- Operating Systems (2003) by Deitel, Deitel, and Choffnes
- Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security) by Albert Marcella Jr. , Doug Menendez
- Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspective by Raghu Santanam (Arizona State University, USA), M. Sethumadhavan (Amrita University, India) and Mohit Virendra (Brocade Communications Systems, USA)

- Operating System Security by Trent Jaeger
- Operating System Forensics by Ric Messier

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://www.kali.org/
4. https://nmap.org/
5. https://nmap.org/book/zenmap.html

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	12	15
2	14	15
3	24	30
4	14	20
5	20	20
Total	**84**	**100**

1.4 Fundamentals of Web Application and Security

L	T	P
6	0	4

RATIONALE

Moving beyond the network the most important component any technology stack is the software that lies on top of the infrastructure. We will start with the requirements of how software applications are built, where students need to understand and build their applications to give the real world feel for how the internet stack is working, as well as coding itself. along with showing them real loopholes while coding himself so that they understand the real-world attacks which are possible on applications, and simulate them so that they can come to conclusions and understand the best practices involved in web application security.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the basics of web development using PHP.
- Setup the XAMPP Server environment and vulnerability assessment.
- Understand the strategy behind web-based attacks and their prevention.
- Learn web application penetration testing and ethical hacking.
- Web application penetration testing is comprised of four main steps including information gathering, research and exploitation.
- Learn Advanced MySQL and MS SQL Exploitation along with basic web-based attacks using open-source tools.

DETAILED CONTENTS

Unit I: Web Designing and Penetration Testing (20 Periods)

Process Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis. PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering (14 Periods)

HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit III: Web Application Attacks Part I: (15 Periods)

SQL Injections & Cross Site Scripting SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation.

Unit IV: Web Application Attacks Part II: (15 Periods)

Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation, Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA.

Unit V: Web Application Attacks Part III (20 Periods)

Insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

List of Practical's

- Vulnerability assessment using OpenVAS.
- Vulnerability testing using Nikto.
- Setting up a XAMPP Server.
- Scripting Exercises using PHP.
- Cross-site scripting using OWASP.
- Broken Authentication & Session Management using OWASP.
- Understanding & Preventing SQL Injection.
- Identifying Authentication Bypass.
- Understanding Malicious File Execution Protection.

INSTRUCTONAL STRATEGY

Since this subject is practical oriented, the teacher should demonstrate the capabilities of different security techniques to students while doing practical exercises. The students should be made familiar with web application attacks and related security & prevention tools and techniques.

MEANS OF ASSESSMENT

- Assignment & Quiz,
- Mid-Term and End-Term written test,
- Actual Lab & Practical Work, Viva-voce

Reference Books:

1. Shema, M. & Adam. (2010). Seven deadliest web application attacks. Amsterdam: Syngress Media.

2. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed). Indianapolis, IN: Wiley, John & Sons.

3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). Web application obfuscation. Amsterdam: Syngress Media,U.S.

4. Sullivan, Bryan (2012). Web Application Security, A Beginner's Guide. McGraw- Hill Education.

Websites for Reference:

- http://swayam.gov.in
- http://spoken-tutorial.org
- https://www.kali.org/tools/nikto/
- https://openvas.org/
- https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	20	20
2	14	20
3	15	20
4	15	20
5	20	20
Total	**84**	**100**

1.5 Project-I

L	T	P
0	0	4

- **Rules for the Project:**

- The students would develop their project individually and get the topic approved.
- The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover, they have to submit the progress reports with the final project report at the time of external examination.
- The students will write project proposal and literature survey report in this semester.
- Students will learn various tools used in cyber security and forensics and they will write a report on tools/language learned for final project implementation in second semester.

Tools: NET Tools, KALI, Recuva, Test disk, TOR, Wireshark, Metaspoilt, Cain & Able and other open-source tools used for cyber security.

II Semester

2.1 Cryptography

L	T	P
6	0	6

RATIONALE

After securing the System, OS and Network, It is necessary to secure the communication between multiple devices using the techniques known as cryptography. It is the mechanism using which the information is hidden from public eye and is something which is used very popular across the internet. Therefore, this paper starts with fundamentals of what is cryptography and how cryptography algorithms work and then describes real world scenarios on how data is being processed currently on the internet and how to make it secure from the eyes of an intruder. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the concepts of cryptography.
- Understand different classical ciphers used for cryptography.
- Differentiate between Symmetric and Asymmetric Key Cryptographic Techniques.
- Understand different Public Key cryptosystem algorithms.
- Understand the concept and usage of Cryptocurrency.
- Understand different Authentication Techniques & Protocols.

DETAILED CONTENTS

Unit I: - Classical Ciphers **(12 Periods)**

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher. Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit II: Secret Key Cryptography **(20 Periods)**

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography **(20 Periods)**

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.

Unit IV: Cryptocurrency (12 Periods)

Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit V: Message authentication code and Hash Functions (20 Periods)

Message authentication code Authentication functions, Hash functions- Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

List of Practical's

- To create a simple digital signature by using open-source software/website.
- To understand the process of creating simple digital certificate.
- To understand Public Key Cryptosystem (PKCS v1.5) scheme.
- To implement the following Substitution & Transposition Techniques concepts:

  a) Caesar Cipher
  b) Playfair Cipher
  c) Hill Cipher
  d) Vigenere Cipher
  e) Rail fence – Row & Column Transformation

- To implement the following algorithms

  a) DES
  b) RSA Algorithm
  c) Diffiee-Hellman
  d) MD5
  e) SHA-1

INSTRUCTONAL STRATEGY

Explanation of concepts using real time examples, diagrams etc. For practical sessions teacher may use simulator software to demonstrate various scenarios related to cryptography.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Actual laboratory and practical work, exercises and viva-voce
- Software installation, operation and viva-voce

Reference Books:

1. Delfs, H. & Knebl, H. (2001). Introduction to Cryptography: Principles and Applications. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). Cryptography and network security: Principles and practice (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). The Handbook of Applied Cryptography. CRC Press.

4. Schneier, B. (1995). Applied cryptography, Protocols, algorithms and source code in C (2nd ed.). New York: John Wiley & Sons.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Websites for Reference:

- http://swayam.gov.in
- http://spoken-tutorial.org
- https://nptel.ac.in/
- https://cse29-iiith.vlabs.ac.in/

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	**Time Allotted (Periods)**	**Marks Allotted (%)**
1	12	15
2	20	25
3	20	25
4	12	10
5	20	25
Total	**84**	**100**

2.2 Cyber Crime, Laws & Forensic Investigation

L	T	P
6	0	0

RATIONALE

This paper focuses on the basic understanding and awareness of cybercrimes and cyber security laws to the professionals learning the cyber security and ethical hacking techniques. This paper addresses and emphasise on the activities leading to infringement of individual or organisational privacy. Further, the paper intends to create highly sensitised professionals who would be responsible for carefully handling the issues related to cyber security in different domains and diligently dealing with forensics.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the types of cyber-crimes, issues and security policies.
- Understand the Cyber Laws & IT Act 2000 framework in India.
- Understand the categorization of various offences & penalties.
- Understand the steps of recording forensic investigation.

DETAILED CONTENTS

Unit 1. Cyber Crime & Issues: **(20 Period)**

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses, Ethical issues in IT, Ethical Conducts, technology trends that raise ethical issues.

Unit 2. Security Policies: **(12 Period)**

Need for an Information Security Policy, Information Security Standards-ISO, WWW policy, Email Security policy, corporate policy, sample security policy, Policy Review Process

Unit 3. Cyber Laws and Regulatory Framework of Information and Technology Act 2000:

(20 Period)

Cyber Laws: Need for Cyber Laws, Copyright Act, Patent Law, IPR, Intellectual Property Law: Copy Right Law, Software License, Semiconductor Law and Patent Law, Software License.

Regulatory Framework: Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. (Rules announced under the Act)

Unit 4. Offenses & Penalties: **(12 Periods)**

Offences under the Information and Technology Act 2000 & it's amendments, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed). Limitations of Cyber Law.

Unit 5. Cyber Forensics Investigation **(20 Periods)**

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems, Hashcat. Work on open Source, Commercial tools and Cyber range.

INSTRUCTONAL STRATEGY

The content of this course is to be taught on conceptual basis with real world examples. Since this subject is theory oriented, the teacher should illustrate the concepts with real life-based case studies. The students should be made familiar with various terminologies related to Cyber world.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Case Studies and Judgements.

Reference Books:

- Kamath, N. (2004). Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.). Delhi: Universal Law Publishing Co.
- Sharma J. P, & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt. Ltd.
- Paintal, D. Law of Information Technology. New Delhi: Taxmann Publications Pvt. Ltd.
- Stephenson, P.R. & Gilbert, K. Investigating computer- related crime a handbook for corporate investigators. Boca Raton, FL: Taylor & Francis.
- Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.
- K.Mani, A Practical Approach to Cyber Laws.
- Tripathi S.P., Introduction to Information Security & Cyber Laws

Websites for Reference:

- http://swayam.gov.in

- http://spoken-tutorial.org
- https://www.meity.gov.in/content/cyber-laws

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	**Time Allotted (Periods)**	**Marks Allotted (%)**
1	20	20
2	12	15
3	20	25
4	12	15
5	20	25
Total	**84**	**100**

2.3 Mobile Concepts & Security

L	T	P
4	0	6

RATIONALE

In today's world, when organizations are preferring not only the web-based approach but also mobile based approach for their business and communication. The cell phone revolution has hit both the enterprise and the consumer market in a massive way. It is required to carefully understand the entire cell phone domain and eco-system, and the possibility of various attacks at each stage needs to be practically performed and critically evaluated in order to understanding how to develop a protected mobility system, which is going to be one of the most important pillars to transform an organisation into a digital organisation.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the fundamentals of mobile system and its security.
- Understand the technologies used in a mobile based approach.
- Understand the types & working of various mobile networks.
- Know the tools & various technologies used for mobile management and security.
- Understand various types of attacks by testing different mobile OS.

DETAILED CONTENTS

Unit I: Introduction to Mobile Concepts & Security (06 Periods)

Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile System Technology (10 Periods)

Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery.

Unit III: Mobile Networks (15 Periods)

Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, VoLTE and its working, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications

Unit IV: Mobility Management (15 Periods)

Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools.

Unit V: Scenario Testing (10 Periods)

Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS

List of Practical's

- To understand various types of Cellular Attacks
- To identify WEP/WPA attacks.
- To understand mobile crypto algorithms.
- To use mobile management tools.
- To implement the mobile backup & data recovery using open-source tools.
- To use mobile vulnerability assessment tools.
- To do mobile testing using open source tools like Monkey Talk, Appium, Katalan Studio.
- To use the container technologies.

INSTRUCTONAL STRATEGY

Explanation of concepts using real time examples, diagrams etc. For practical sessions demonstration of various simulators are required. Various exercises and small applications should be given along with theoretical explanation of concepts.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Actual laboratory and practical work, exercises and viva-voce
- Software installation, operation and viva-voce

Reference Books:

1. Fried, S. (2010). Mobile device security: A comprehensive guide to securing your information in a moving world. Boca Raton, FL: Auerbach Publications.

2. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed.). Indianapolis, IN: Wiley, John & Sons.

3. Dwivedi, H., Clark, C., & Thiel, D. (2010). Mobile application security. New York: McGraw-Hill Companies.

Websites for Reference:

- http://swayam.gov.in
- http://spoken-tutorial.org
- https://developer.android.com/training/articles/security-tips

- https://developer.apple.com/documentation/security
- https://en.wikipedia.org/wiki/Mobile_security

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	06	10
2	10	20
3	15	25
4	15	25
5	10	20
Total	**56**	**100**

2.4 Seminar: Paper Presentation

L	T	P
0	0	2

Guidelines:

The following rules and guidelines apply:

- The student should let the course faculty know in advance the intended topic of the seminar. This is just to avoid the situation that two students give a seminar on the very same topic.
- The Topic should be related to cyber security & related field.
- The length of the seminar should be at most 20 minutes, including time at the end for questions from the audience. The minimum length is 15 minutes, excluding questions at the end.
- Each seminar should be given by one single student. Two students may still work together on a project and then give a tandem presentation consisting of two consecutive seminars.
- The intended audience for the seminar is other students attending the course. Prepare the seminar accordingly.

Suggestive Evaluation:

Planned learning outcomes	**Level of attainment (Marking Scale)**	**Faculty's comments**
Academic content	High Average Low	
Knowledge and understanding of core material	10 9 8 7 6 5 4 3 2 1	
Extent, quality and appropriateness of research	10 9 8 7 6 5 4 3 2 1	
Conceptual grasp of issues, quality of argument and ability to answer questions	10 9 8 7 6 5 4 3 2 1	
Quality of management	High Average Low	
Pacing of presentation	10 9 8 7 6 5 4 3 2 1	
Effective use of visual material -whiteboard, visual aids, handouts (as appropriate)	10 9 8 7 6 5 4 3 2 1	
Organisation/structure of material (intro; main body; conclusion)	10 9 8 7 6 5 4 3 2 1	

Quality of communication	High Average Low	
Audibility, liveliness and clarity of presentation	10 9 8 7 6 5 4 3 2 1	
Confidence and fluency in use of English	10 9 8 7 6 5 4 3 2 1	
Appropriate use of body language (inc. eye contact)	10 9 8 7 6 5 4 3 2 1	
Listening skills: responsiveness to audience	10 9 8 7 6 5 4 3 2 1	
Summative comment:		

2.5 Project-II

L	T	P
0	0	6

Rules for the Project:

● The students would develop their project individually on the topic approved in first semester.

● The students have to report to the guide for at least five times during the project lifespan with the progress report duly signed by the internal guide. Moreover, they have to submit the progress reports with the final project report at the time of external examination.

● The evaluation must be based on the project report and the seminars.

A suggestive criterion for assessing student performance by the external (personnel from industry) and internal (teacher) examiner is given in table below:

Sr. No	Performance criteria	Max.** marks	Rating Scale				
			Excellent	**Very Good**	**Good**	**Fair**	**Poor**
1.	Selection of project assignment	10	10	8	6	4	2
2.	Planning and execution of considerations	10	10	8	6	4	2
3.	Quality of performance	20	20	16	12	8	4
4.	Providing solution of the problems or production of final product	20	20	16	12	8	4
5.	Sense of responsibility	10	10	8	6	4	2
6.	Self-expression/ communication skills	5	5	4	3	2	1
7.	Interpersonal skills/human relations	5	5	4	3	2	1
8.	Report writing skills	10	10	8	6	4	2
9.	Viva voce	10	10	8	6	4	2
Total marks		**100**	**100**	**80**	**60**	**40**	**20**

The overall grading of the practical training shall be made as per following table

	Range of maximum marks	Overall grades
i)	More than 80	Excellent
ii)	79 <> 65	Very good
iii)	64 <> 50	Good
iv)	49 <> 40	Fair
v)	Less than 40	Poor

In order to qualify for the diploma, students must get “Overall Good grade” failing which the students may be given one more chance of undergoing 8 -10 weeks of project oriented professional training in the same industry and re-evaluated before being disqualified and declared “not eligible to receive diploma”. It is also important to note that the students must get more than six “goods” or above “good” grade in different performance criteria items in order to get “Overall Good” grade.

Important Notes

- **These criteria must be followed by the internal and external examiner and they should see the daily, weekly and monthly reports while awarding marks as per the above criteria.**
- **The criteria for evaluation of the students have been worked out for 100 maximum marks. The internal and external examiners will evaluate students separately and give marks as per the study and evaluation scheme of examination.**
- **The external examiner, preferably, a person from industry/organization, who has been associated with the project-oriented professional training of the students, should evaluate the students’ performance as per the above criteria.**
- **It is also proposed that two students or two projects which are rated best be given merit certificate at the time of annual day of the institute. It would be better if specific nearby industries are approached for instituting such awards.**

The teachers are free to evolve another criterion of assessment, depending upon the type of project work.

The students must submit a project report of not less than 30 pages (excluding coding). The report must follow the Cyber Security Concepts.

It is proposed that the institute may organize an annual exhibition of the project work done by the students and invite leading Industrial organizations in such an exhibition. It is also proposed that two students or two projects which are rated best be given merit certificate at the time of annual day of the institute. It would be better if specific industries are approached for instituting such awards.

10. RESOURCE REQUIREMENT

10.1 Physical Resources

10.1.1 Space Requirement:

Norms and standards laid down by All India Council for Technical Education (AICTE) may be followed to work out space requirement in respect of class rooms, tutorial rooms, drawing halls, laboratories, space required for faculty, student amenities and residential area for staff and students.

10.1.2 Laboratoires/Shops

- Cyber Security Lab

Cyber Security Lab			
1.	Computer Server (Quad core, intel processor 32 GB RAM, Windows Server16 or higher)	1	10,00,000/-
2.	Computer Desktop (i7, Latest Generation, 512SSD/1TB Hard disk, 8GB RAM, Linux OS, 3 years warranty)	20	16,00,000/-
3.	Computer Desktop (i7, Latest Generation, 512SSD/1TB Hard disk, 8GB RAM, Windows OS 10/11 or latest, 3 years warranty)	20	16,00,000/-
4.	Online UPS, 6KVA with battery Warranty on UPS-3 Years Warranty on Battery-36 Months	1	1,50,000/-
5.	Switch with 48 port speed 10/100/1000 (Manageable)	1	70,000/-
6.	WIFI Modem or Router	5	10,000/-
7.	Connectors (RJ-45, RJ-11, BNC, SC, ST)	LS	10,000/-
8.	Cables: (UTP, STP, OFC) - 25 m each	LS	10,000/-
9.	Multifunctional Laser/Ink tank Printer	1	30,000/-
10.	Router	1	40,000/-
11.	Modem cum Router	2	10,000/-
12.	Compact Disk/DVD R/W	100	2000/-
13.	External Hard Disk	4	30,000/-
14.	Internet Connectivity	40 Nodes	1,00,000/-
15.	Unmanaged Switch	4	60,000/-
16.	Hardware based Firewall	1	2,50,000/-

17.	Video Conferencing System	1	2,00,000/-
18.	Green Air Conditioner-2 ton with stabilizer	2	1,00,000/-
19.	Miscellaneous- cables and connectors, computer stationery, printer consumables (inks), toner etc.	LS	30,000/-
20.	LCD/DLP Projector with Screen (Full HD or higher with at least 3200 Lumens)	1	1,00,000/-
21.	Libre Office/Open Office (Freeware)	-	-
22.	Kali Linux(Freeware)	-	-
23.	Nmap/ZENMAP Metasploit Wireshark OWASP OpenVAS NET Tools, Test disk, TOR, Cain & Able and other open-source tools used for cyber security as mentioned/required in the curriculum	-	-

10.1.3 Furniture Requirement

1. Norms and standards laid down by AICTE be followed for working out furniture requirement for this course.

2. Furniture for laboratories/Computer Centre 15 lacs

10.2 Human Resources

3. Weekly work schedule, annual work schedule, student teacher ratio for various group and class size, staffing pattern, work load norms, qualifications, experience and job description of teaching staff workshop staff and other administrative and supporting staff be worked out as per norms and standards laid down by the AICTE. The website www.aicte.ernet.in may be referred for downloading current norms and standards pertaining to technician courses.

11. EVALUATION STRATEGY

11.1 INTRODUCTION

Evaluation plays an important role in the teaching-learning process. The major objective of any teaching-learning endeavour is to ensure the quality of the product which can be accessed through learner's evaluation.

The purpose of student evaluation is to determine the extent to which the general and the specific objectives of curriculum have been achieved. Student evaluation is also important from the point of view of ascertaining the quality of instructional processes and to get feedback for curriculum improvement. It helps the teachers in determining the level of appropriateness of teaching experiences provided to learners to meet their individual and professional needs. Evaluation also helps in diagnosing learning difficulties of the students. Evaluation is of two types: Formative and Summative (Internal and External Evaluation)

Formative Evaluation

It is an on-going evaluation process. Its purpose is to provide continuous and comprehensive feedback to students and teachers concerning teaching-learning process. It provides corrective steps to be taken to account for curricular as well as co-curricular aspects.

Summative Evaluation

It is carried out at the end of a unit of instruction like topic, subject, semester or year. The main purpose of summative evaluation is to measure achievement for assigning course grades, certification of students and ascertaining accountability of instructional process. The student evaluation has to be done in a comprehensive and systematic manner since any mistake or lacuna is likely to affect the future of students.

In the present educational scenario in India, where summative evaluation plays an important role in educational process, there is a need to improve the standard of summative evaluation with a view to bring validity and reliability in the end-term examination system for achieving objectivity and efficiency in evaluation.

11.2 STUDENTS' EVALUATION AREAS

The student evaluation is carried out for the following areas:

- Theory
- Practical Work (Laboratory, Workshop, Field Exercises)
- Project Work
- Professional Industrial Training

A. Theory

Evaluation in theory aims at assessing students' understanding of concepts, principles and procedures related to a course/subject, and their ability to apply learnt principles and solve problems. The formative evaluation for theory subjects may be caused through sessional /class-tests, home-assignments, tutorial-work, seminars, and group discussions etc. For end-term evaluation of theory, the question paper may comprise of three sections.

Section-I

It should contain objective type items e.g., multiple choice, matching and completion type. Total weightage to Section-1 should be of the order of 20 percent of the total marks and no choice should be given in this section. The objective type items should be used to evaluate students' performance in knowledge, comprehension and at the most application domains only.

Section-II

It should contain short answer/completion items. The weightage to this section should be of the order of 40 percent of the total marks. Again, no choice should be given in section-II

Section-III

It may contain two to three essay type questions. Total weightage to this section should be of the order of 40 percent of the total marks. Some built-in, internal choice of about 50 percent of the questions set, can be given in this section

Table II: Suggested Weightage to be given to different ability levels

Abilities	Weightage to be assigned
Knowledge	10-30 percent
Comprehension	40-60 percent
Application	20-30 percent
Higher than application i.e., Analysis, Synthesis and Evaluation	Up to 10 percent

B. Practical Work

Evaluation of student's performance in practical work (Laboratory experiments, Workshop practical's/field exercises) aims at assessing students' ability to apply or practice learnt concepts, principles and procedures, manipulative skills, ability to observe and record, ability to interpret and draw conclusions and work-related attitudes. Formative and summative evaluation may comprise of weightages to performance on task, quality of product, general behaviour and it should be followed by viva-voce.

C. Project

The purpose of evaluation of project work is to assess students' ability to apply, in an integrated manner, learnt knowledge and skills in solving real life problems, manipulative skills, ability to observe, record, creativity and communication skills. The formative and summative evaluation may comprise of weightage to nature of project, quality of product, quality of report and quality of presentation followed by viva-voce.

11.3 ASPECTS OF QUESTION PAPER SETTING

Validity and reliability are the most important considerations in the selection and construction of evaluation procedures. First and foremost are the evaluation tools to measure the specific outcomes for which they are intended to measure. Next in importance is reliability, and following that is a host of practical features that can be classified under the heading of usability.

For weightage of marks assigned to formative (internal) and summative (external) evaluation and duration of evaluation has been given in the study and evaluation scheme of the curriculum document. Teachers/Paper-setters/Examiners may use Manual for Students' Evaluation developed by Institute of Research Development & Training, U.P. Kanpur to bring objectivity in the evaluation system. The working group found it very difficult to detail out precisely the contents of subject on languages and therefore teachers may send guidelines to respective examiners for paper setting to maintain objectivity in evaluation.

12. RECOMMENDATIONS FOR EFFECTIVE CURRICULUM IMPLEMENTATION

This curriculum document is a Plan of Action (POA) and has been prepared based on exhaustive exercise of curriculum planning and design. The representative sample comprising selected senior personnel (lecturers and HODs) from various institutions and experts from industry/field have been involved in curriculum design process.

The document so prepared is now ready for its implementation. It is the faculty of polytechnics who have to play a vital role in planning instructional experiences for the courses in four different environments viz. class-room, laboratory, library and field and execute them in right perspective. It is emphasized that a proper mix of different teaching methods in all these places of instruction only can bring the changes in stipulated students' behaviour as in the curriculum document. It is important for the teachers to understand curriculum document holistically and further be aware of intricacies of teaching-learning process (T-L) for achieving curriculum objectives. Given below are certain suggestions which may help the teachers in planning and designing learning experiences effectively. These are indicative in nature and teachers using their creativity can further develop/refine them. The designers of the programme suggest every course teacher to read them carefully, comprehend and start using them.

(A) Broad Suggestions:

1. Curriculum implementation takes place at programme, course and class-room level respectively and synchronization among them is required for its success. The first step towards achieving synchronization is to read curriculum document holistically and understand its rationale and philosophy.

2. Uttar Pradesh State Board of Technical Education (BTE U.P.) may make the academic plan available to all polytechnics well in advance. The principals have a great role to play in its dissemination and, percolation up to grass-root level. Polytechnics in turn are supposed to prepare institutional academic plan by referring state level BTE plan.

3. HOD of every Programme Department along with HODs and in-charges of other departments are required to prepare academic plan at department level referring institutional academic plan.

4. All lecturers/Senior lecturers are required to prepare course level and class level lesson plans
   referring departmental academic plan.

(B) Course Level Suggestions

Teachers are educational managers at class room level and their success in achieving course level objectives lies in using course plan and their judicious execution which is very important for the success of programme by achieving its objectives.

Polytechnic teachers are required to plan various instructional experiences viz. theory lecture, expert lectures, lab/workshop practical's, guided library exercises, field visits, study tours, camps etc. In addition, they have to carry out progressive assessment of theory, assignments, library, practicals and field experiences. Teachers are also required to do all these activities within a stipulated period of 16 weeks which is made available to them in the academic plan at BTE level. With the amount of time to their credit, it is essential for them to use it judiciously by planning all above activities properly and ensure execution of the plan effectively.

Following is the gist of suggestions for subject teachers to carry out T-L process effectively:

1. Teachers are required to prepare a course plan, taking into account departmental academic plan, number of weeks available, course to be taught, different learning experiences required to be developed etc.

2. Teachers are required to prepare lesson plan for every theory class. This plan may comprise of content to be covered, learning material (transparencies, VCDs, Models etc.)

for execution of a lesson plan. They may follow steps for preparing lesson plan e.g., drawing attention, state instructional objectives, help in recalling pre-requisite knowledge, deliver planned subject content, check desired learning outcome and reinforce learning etc.

3. Teachers are required to plan for expert lectures from field/industry. Necessary steps are to plan in advance, identify field experts, make correspondence to invite them, take necessary budgetary approval etc.

4. Teachers are required to plan for guided library exercises by identification of course specific experience requirement, setting time, assessment, etc. The tutorial, assignment and seminar can be thought of as terminal outcome of library experiences.

5. Concept and content-based field visits with appropriate releases (day-block) may be planned and executed for such content of course which otherwise is abstract in nature and no other requisite resources are readily available in institute to impart them effectively.

6. There is a dire need for planning practical experiences in right perspective. These slots in a course are the avenues to use problem-based learning/activity learning/ experiential learning approach effectively. The development of lab instruction sheets for the course is a good beginning to provide lab experiences effectively.

7. Planning of progressive assessment encompasses periodical assessment in semester, preparation of proper quality question paper, assessment of answer sheets immediately and giving constructive explicit feedback to every student. It has to be planned properly; otherwise, very purpose of the same is lost.

8. The co-curricular activities like camp, social gathering, study tour, hobby club etc. may be used to develop generic skills like task management, problem solving, managing self, collaborating with others etc.

9. Where ever possible, it is essential to use activity-based learning rather than relying on delivery based conventional teaching all the time.

10. While imparting instructions, emphasis may be laid on the development of cognitive, psychomotor, reactive and interactive skills in the students.

11. Teachers may take working drawings from the industry/field and provide practices in reading these drawings.

12. Considerable emphasis should be laid in discipline specific contracting and repair and maintenance of machines, tools and installations.

13. Teachers may take initiative in establishing liaison with industries and field organizations for imparting field experiences to their students.

14. Case studies and assignments may be given to students for understanding of Enterprise Resource Management (ERM).

15. Students be made aware about issues related to ecology and environment, safety, concern for wastage of energy and other resources etc.

16. Students may be given relevant and well thought out minor and major project assignments, which are purposeful and develop practical skills. This will help students in developing creativity and confidence for their gainful employment (wage and self).

17. A Project bank may be developed by the concerned department of the polytechnics in consultation with related Industry, Research Institutes and other relevant field organizations in the state.

List of Participants

Workshops were organised at IRDT Kanpur to develop the Curriculum Contents newly introduced course of PG Diploma in Cyber Security for Board of Technical Education, U.P.

Following experts and reviewers were involved in developing the curriculum contents:

1. Sh. F.R. Khan, Principal Headquarters, Directorate of Technical Education, Kanpur.
2. Sh. Ashok Kushwaha, Principal GGP Risia Nanpara Bahraich.
3. Sh. Madan Mishra, HOD Computer Science, MMIT Sant Kabir Nagar.
4. Sh. Pawan Kumar Gupta, HOD, IT, CMS GGP Daurala Meerut.
5. Sh. Lalit Kumar Gupta, Lecturer, IT, MMIT Amroha.
6. Ms. Fatema Siddiqua, Lecturer, CS, Government Polytechnic, Ghaziabad.
7. Sh. Sheetanshu Krishna, Lecturer, CS, Govt. Girls Polytechnic, Amethi.
8. Mr. Nasir Hussain, Barclays, Manchester, United Kingdom.
9. Sh. Devinder M. Saini, TBRL, DRDO, Chandigarh.
10. Ms. Mugdha Tripathi, WIPRO Ltd., Bangalore.
11. Sh. Gaurav Kishor Kanaujiya, Assistant Professor, IRDT Kanpur.

Curriculum Designed by

Institute of Research Development & Training

U.P. Kanpur