SAVITRIBAI PHULE PUNE UNIVERSITY PUNE
CHOICE BASED CREDIT SYSTEM

For

M.Sc.(Cyber Security)

(Implemented from June 2024)

Title of the Course: M.Sc. (Cyber Security)

Preamble

The Master of Science in Cyber Security (M.Sc. Cyber Security) program is designed to provide advanced education and training in the field of Cyber Security. This comprehensive program aims to equip students with a profound understanding of theoretical concepts, practical skills, and cutting-edge technologies relevant to the rapidly evolving world of computing.

With a strong emphasis on academic excellence and research-driven learning, the M.Sc. Cyber Security program seeks to nurture a community of skilled Cyber security professionals capable of addressing complex challenges across various industries. By fostering a stimulating and innovative learning environment, we strive to empower our students to become leaders, innovators, and agents of positive change in the field of Computer Science.

Eligibility

(a) B.Sc.(Cyber and Digital Science) OR
(b) B.Sc. (Cyber Security)
(c) Bachelor of Computer Science (B.C.S.) OR
(d) B.Sc.(Computer Science) OR
(e) B.C.A.(Science) OR
(f) B.Sc.(Information Technology) OR
(g) B.Sc. (Cloud Computing) OR
(h) Bachelor of Engineering(BE) in Computer Science/Information Technology/Electronics and Telecommunication/AI and Data Science/AI and Machine Learning/ equivalent OR
(i) B.Voc. in Software Development/ Information Technology
(j) B.Sc. with Computer Science as Principal Subject
(k) General B.Sc. with Computer Science as one of the subject at TYBSc level OR
Graduate degree from a recognized university / institution with an equivalent qualification.

PO No	Outcomes
PO 1	In today's IT environment, recognize and apply wireless security.
PO 2	Protect and defend computer systems and networks from Cybersecurity threats.
PO 3	Learn innovative abilities to tackle modern cyber security tasks like Vulnerability assessment and penetration testing.
PO 4	Understand advanced malware analysis, IT laws, digital payments, and Security concepts.
PO 5	Students are able to present information security solutions to both technical And non-technical decision-makers both orally and in writing.
PO 6	Students are able to recognize and evaluate the dangers, threats, and Weaknesses related to technological devices.
PO 7	Understand new tools and technologies which are trending
PO 8	Understand the working of Virtualization &Security Audit
PO 9	Students can create reports summarizing their research and providing Concept proof.
PO 10	Students can understand cloud services, applications, and security.

Savitribai Phule Pune University

Syllabus Structure as per NEP Guidelines

M.Sc.(Cyber Security)from2024-25 SEMESTER I

Course Type	Course Code	Course Code	Course Title		Teaching Scheme Hr/Week		Evaluation Scheme and Max Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core (10+4)	MCS-501-MJ	Malware Analysis II	2		2		15	35	50
	MCS-502-MJ	Intrusion Detection and Prevention System	2		2		15	35	50
	MCS-503-MJ	Digital Image Processing	2		2		15	35	50
	MCS-504-MJP	PracticalBasedonMCS501MJ		2		4	15	35	50
	MCS-505-MJP	PracticalBasedonMCS502MJ		2		4	15	35	50
Major Elective (2+2)	MCS-510-MJ	Digital Payments and Its Security	2		2		15	35	50
	MCS-511-MJP	PracticalBasedonMCS510MJ		2		4	15	35	50
	OR								
	MCS-512-MJ	Wireless Security	2		2		15	35	50
	MCS-513-MJP	PracticalBasedonMCS512MJ		2		4	15	35	50
	OR								
	MCS-514-MJ	ITAct2000inCyberspace	2		2		15	35	50
	MCS-515-MJP	PracticalBasedonMCS514MJ		2		4	15	35	50
Minor(4)	MCS-531-RM	Research Methodology	4		4		30	70	100
		TOTAL	**16**	**6**					

SEMESTERII

Course Type	Course code	Course Name	Credits		Teaching Scheme Hrs/Week		Examination Scheme and Marks		
			TH	**PR**	**TH**	**PR**	**CE**	**EE**	**Total**
Major Core (10+4)	MCS-551-MJ	Mobile Application and Services	2		2		15	35	50
	MCS-552-MJ	Incident Handling	2		2		15	35	50
	MCS-553-MJ	Cyber Security Architecture	2		2		15	35	50
	MCS-554-MJP	Practical Based on MCS551MJ		2		4	15	35	50
	MCS-555-MJP	Practical Based on MCS552MJ		2		4	15	35	50
Major Elective (2+2)	MCS-560-MJ	Dark web and Cyber warfare	2		2		15	35	50
	MCS-561-MJP	Practical Based on MCS560MJ		2		4	15	35	50
	OR								
	MCS-562-MJ	Dev Sec Ops	2		2		15	35	50
	MCS-563-MJP	Practical Based on MCS562MJ		2		4	15	35	50
	OR								
	MCS-564-MJ	Tools and Technology for Cyber Security	2		2		15	35	50
	MCS-565-MJP	Practical Based on MCS - 563-MJ		2		4	15	35	50
FP/OJT/CEP (4)	MCS-581-OJT	OJT		4		8	30	70	100
TOTAL			**12**	**10**					

SEMESTERIII

Course Type	Course code	Course Name	Credits		Teaching Scheme Hrs/Week		Examination Scheme and Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	MCS-601-MJ	Cloud Security and Services	4	-	4	--	30	70	100
	MCS-602-MJ	Virtualization &Forensics	4	-	4	--	30	70	100
	MCS-603-MJ	Security Audit	2	-	2	--	15	35	50
	MCS-604-MJP	LabcourseonMCS-601-MJ and 603	-	2	--	4	15	35	50
	MCS-605-MJP	LabcourseMCS-602-MJ	-	2	--	4	15	35	50
Major Elective	MCS-610-MJ	Penetration Testing	2	-	2	--	15	35	50
	MCS-611-MJP	LabCourseonMCS-610-MJ	-	2	--	4	15	35	50
	OR								
	MCS-612-MJ	DevOps Fundamentals	2	-	2	--	15	35	50
	MCS-613-MJP	LabCourseonMCS-612-MJ	-	2	--	4	15	35	50
	OR								
	MCS-614-MJ	Mobile forensic	2	-	2	--	15	35	50
	MCS-615-MJP	PracticalonMCS-614-MJ	-	2	--	4	15	35	50
Research Project	MCS-631-RP	Research Project Work (120 Hrs)	-	4	-	-	30	70	100
		Total	**12**	**10**					

SEMESTERIV

Course Type	Course code	Course Name	Credits		Teaching Scheme Hrs/Week		Examination Scheme And Marks		
			TH	PR	TH	PR	CE	EE	Total
Major Core	MCS-651-MJP	Full Time Industrial Training (IT)	-	12	-	-	90	210	300
Major Elective	MCS-652-MJ	Online/MOOC(Elective Courses List)	4	-	-	-	30	70	100
Research Project	MCS-681-RP	Research Project Work (180 hrs.)	-	6	-	-	45	105	150
		Total	**4**	**18**					

Abbreviations

MCS	MSc Cyber Security	**MJ**	Major Theory
RM	Research Methodology	**MJP**	Major Practical
OJT	On Job Training	**RP**	Research Project
TH	Theory	**PR**	Practical
CE	Continuous Evaluation	**EE**	End semester Evaluation
MOOC	Massive Open Online Course		

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS501MJ
Subject: Malware Analysis II

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Understanding of Windows and Linux operating systems, Malware and Networking, Web and OS security attacks, High Level & Low Level Programming

Course Objectives:-

- Learn to analyze various malicious file types
- Apply various tools to Identify the vulnerabilities and to perform Malware analysis
- Apply malware classification and functionality & anti-reverse engineering techniques

Course Outcomes:-Student will be able to:-

- Learn to analyze various malicious file types
- Apply various tools to Identify the vulnerabilities and to perform Malware analysis
- Apply malware classification and functionality & anti-reverse engineering techniques

Course Contents

Unit 1	**Advanced Dynamic Analysis Techniques**	**5 Hours**

1.1 Behavioral Heuristics in Dynamic Analysis
1.2 Memory Forensics during Dynamic Analysis
  1.2.1 Runtime Code Injection
  1.2.2 Hooking and Detouring
1.3 Advanced Sandboxing Techniques
1.4 Detecting Anti-Analysis Techniques
  1.4.1 Anti-VM
  1.4.2 Anti-Debugging

Unit 2	**Advanced Static Analysis Strategies**	**6 Hours**

2.1 Cryptanalysis and Deobfuscation
2.2 Function Identification and Reconstruction
2.3 Control Flow Analysis
2.4 Automated Malware Classification
 2.4.1 Machine Learning Models
 2.4.2 Feature Extraction

Unit 3	**Malware Reverse Engineering**	**5 Hours**

3.1 Reverse Engineering Fundamentals
3.2 Debugging Malicious Binaries
3.3 Analyzing Encrypted and Packed Malware
3.4 Code Reversing Techniques
  3.4.1 Patching
  3.4.2 Dynamic Analysis Integration

Unit 4	Threat Intelligence Integration	7 Hours
4.1 Role of Threat Intelligence in Malware Analysis 4.2 Incorporating Threat Feeds and Indicators 4.3 Leveraging Open Source Intelligence (OSINT) 4.4 Threat Hunting Techniques 4.4.1 Proactive Analysis 4.4.2 Indicators Correlation		
Unit 5	**Malware Analysis in Networked Environments**	**7 Hours**
5.1 Analyzing Network-based Malware 5.2 Detecting Command and Control (C2) Servers 5.3 Incident Response in Networked Environments 5.4 Collaborative Malware Analysis 5.4.1 Information Sharing Platforms 5.4.2 Joint Analysis Centers (JACs)		
Reference Books:		
• Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware by Monnappa K A • Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks Kindle Edition by Alexey Kleymenov (Author), Amr Thabet (Author) • Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig • Malware, Rootkits & Botnets: A Beginner's GuideChristopher C. Elisan		

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security))
Subject Code : MCS502MJ
Subject: Intrusion Detection and Prevention System

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Knowledge of Cyber Security
- Fundamental knowledge in Operating Systems, and Network.

Course Objectives:-

- Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
- Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.

Course Outcomes:-Student will be able to:-

- Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.
- Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.

Course Contents

Unit 1	**Fundamentals of Intrusion Detection and Prevention**	**4 Hours**

1.1 Introduction to IDS and IPS
1.2 Types of Attacks Detected
1.3 Signatures vs. Anomalies Detection
1.4 Role of Machine Learning in IDS/IPS

Unit 2	**Network and Host based Intrusion Detection Systems**	**8 Hours**

2.1 Architecture of NIDS
2.2 Packet Inspection and Sniffing
2.3 Common NIDS Signatures
 2.3.1 Port Scans
 2.3.2 DDoS Attacks
2.4 Limitations and Challenges in NIDS
2.5 Deploying HIDS on Endpoints
2.6 File Integrity Monitoring
2.7 System Log Analysis
2.8 Anomaly Detection on Hosts
 2.8.1 Behavior Analysis
 2.8.2 User Activity Monitoring

Unit 3	Intrusion Prevention Systems and Advanced Techniques in IPS/ IDS	6 Hours
3.1 IPS Architecture 3.2 Inline vs. Passive IPS 3.3 Stateful Inspection and Deep Packet Inspection 3.4 Blocking and Alerting Mechanisms – 3.5 Heuristic Analysis in Intrusion Detection 3.6 Protocol-based Detection 3.7 SSL/TLS Inspection in IDS/IPS 3.8 Evasion Techniques and Countermeasures		
Unit 4	**Security Information and Event Management (SIEM) Integration**	**4 Hours**
4.1 Correlation and Aggregation in SIEM 4.2 Logging and Event Collection 4.3 Real-time Monitoring with SIEM 4.4 Incident Response Using SIEM		
Unit 5	**Best Practices , Implementation Strategies, Challenges and Future Trends in IDS/IPS**	**8 Hours**
5.1 IDS/IPS Deployment in Enterprise Networks 5.2 Fine-tuning Signatures and Rules 5.3 Regular Updates and Patch Management 5.4 Compliance and Regulatory Considerations 5.1 Overcoming False Positives and Negatives 5.2 Scalability and Performance Challenges 5.3 Cloud-based IDS/IPS Solutions 5.4 Integration with Threat Intelligence Platforms		
Reference Books:		
• INTRUSION DETECTION SYSTEM: An easiest book to learn IDS (Hacking Precautions 2) by Saiful Hasan • Network Intrusion Detection and Prevention: Concepts and Techniques: 47 (Advances in Information Security) by Ali A. Ghorbani, Wei Lu, et al. • The State of the Art in Intrusion Prevention and Detection by Al-Sakib Khan Pathan		

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security))
Subject Code : MCS503MJ
Subject: Digital Image Processing

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

1. Basic Knowledge of Digital Communication

Course Objectives:-

- To learn and understand various image compression and Segmentation used in digital image processing
- To learn and understand various image enhancement technique used in digital image processing

Course Outcomes:-Student will be able to:-

- Develop and implement algorithms for digital image processing.
- Apply image processing algorithms for practical object recognition applications.

Course Contents

Unit 1	**Introduction to Digital Image Processing**	**4 Hours**

1.1 Basics of Digital Images
1.2 Fundamentals of Image Processing
1.3 Image Acquisition and Sampling
1.4 Image Representation and Histograms

Unit 2	**Image Enhancement and Restoration Techniques**	**6 Hours**

2.1 Spatial Domain Methods
2.1.1 Point Operations
2.1.2 Histogram Equalization
2.2 Frequency Domain Methods
2.2.1 Fourier Transform
2.2.2 Filtering Techniques
2.3 Degradation Models
2.4 Noise Removal
2.4.1 Spatial Filtering
2.4.2 Frequency Domain Filters
2.5 Inverse Filtering and Wiener Filtering
2.6 Restoration Evaluation Metrics

Unit 3	Image Compression and Segmentation	6 Hours
3.1 Lossless vs. Lossy Compression 3.2.2 Basics of Image Compression 3.2.1 Run-Length Encoding 3.2.2 Huffman Coding 3.3 Transform Coding and JPEG Compression 3.4 Evaluation of Compression Techniques 3.5 Importance of Image Segmentation 3.6 Thresholding Techniques 3.7 Region-based Segmentation 3.7.1 Region Growing 3.7.2 Split and Merge 3.8 Edge Detection and Boundary Extraction		
Unit 4	**Object Recognition and Classification**	**4 Hours**
4.1 Feature Extraction Methods 4.2Template Matching 4.3 Machine Learning in Image Classification 4.4 Deep Learning Approaches		
Unit 5	**Morphological Image Processing**	**6 Hours**
5.1 Basics of Mathematical Morphology 5.2 Dilation and Erosion Operations 5.3 Opening and Closing Operations 5.4 Applications of Morphological Operations		
Unit 6	**Advanced Topics in Digital Image Processing**	**4 Hours**
6.1 Multispectral and Hyperspectral Imaging 6.2 3D Image Processing 6.3 Image Registration and Fusion 6.4 Emerging Trends in Image Processing Technologies		
Reference Books:		
Fundamentals of Digital Image Processing Paperback – 1 January 2015 by Jain (Author) Digital Image Processing: An Algorithmic Introduction Using Java (Texts in Computer Science) Hardcover – 19 January 2012 by Wilhelm Burger (Author), Mark J. Burge (Author) Digital Image Processing: An Algorithmic Introduction Using Java (Texts in Computer Science) Hardcover – 19 January 2012 by Wilhelm Burger (Author), Mark J. Burge (Author)		

MCS-504MJP : Practical Based on MCS501MJ		
Teaching Scheme 2 hours / week	**No. of Credits: 2**	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:

1. Basic Python Programming
2. Basic Computer Hardware
3. Basic Assembly Programming

Course Objectives: -

1. Static and Dynamic Analysis of Malwares
2. Study of windows malwares in depth.
3. Study of linux malwares, Mac malwares, Android malware in brief

Course Outcomes: - Student will be able to :-

1. Classify the malwares and analyze them.
2. Use the tools for analysis of any type of malware.
3. Write own tools/programs for analyzing the malware

Practical List

Assignment No 1

- How do you configure an intrusion detection system (IDS) to effectively monitor network traffic for potential security threats?

Assignment No 2

- Can you explain the role of signatures in an intrusion prevention system (IPS), and how do you update them to enhance security?

Assignment No 3

- 3. What are the key differences between host-based and network-based intrusion detection systems, and when might you choose one over the other?

Assignment No 4

- Describe a scenario where an IDS alerts on a potential security incident. What steps would you take to investigate and respond to this alert?

Assignment No 4

- How do you ensure the proper tuning of an intrusion detection and prevention system to minimize false positives and negatives while maintaining a high level of security?

Malware Sources

Hybrid Analysis: https:/ / www. hybrid- analysis. com/
KernelMode.info: http:/ / www. kernelmode. info/ forum/ viewforum. php? f= 16
VirusBay:https:/ / beta. virusbay. io/
Contagio malware dump:http:/ / contagiodump. blogspot. com/
AVCaesar:https:/ / avcaesar. malware. lu/
Malwr:https:/ / malwr. com/
VirusShare:https:/ / virusshare. com/
theZoo:http:/ / thezoo. morirt. com/
https://zeltser.com/malware-sample-sources/

MCS-505-MJP: Practical Based on MCS 502MJ
Intrusion Detection and Prevention System

Teaching Scheme	**No. of Credits:2**	**Examination Scheme**
2 hours / week		CA :15 marks UA: 35 marks

Prerequisites:
1. Fundamentals of Cyber Security

Course Objectives: -

- Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
- Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.

Course Outcomes: - Student will be able to :- 1.

- Understand the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.
- Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.

Practical List

Assignment No 1

- How do you configure an intrusion detection system (IDS) to effectively monitor network traffic for potential security threats?

Assignment No 2

- Can you explain the role of signatures in an intrusion prevention system (IPS), and how do you update them to enhance security?

Assignment No 3

- What are the key differences between host-based and network-based intrusion detection systems, and when might you choose one over the other?

Assignment No 4

- Describe a scenario where an IDS alerts on a potential security incident. What steps would you take to investigate and respond to this alert?

Assignment No 5

- How do you ensure the proper tuning of an intrusion detection and prevention system to minimize false positives and negatives while maintaining a high level of security?

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security))
Subject Code : MCS-510-MJ
Subject: Digital Payments & Security

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Knowledge of digital payments & Gateways

Course Objectives:-

- To provide adequate knowledge and understanding about Digital Payments with the security to the students
- The technologies facilitating Digital Payments and different platforms.

Course Outcomes:-Student will be able to:-

- To Analyse the impact of Digital Payments and its security on business models and strategy
- Explain the process that should be followed while making online payments

Course Contents

Unit 1	**Introduction to Digital Payments and Technologies Infrastructure**	**8 Hours**

1.1 Evolution of Digital Payments
1.2 Types of Digital Payment Systems
1.2.1 Mobile Payments
1.2.2 Online Banking
1.2.3 Cryptocurrencies
1.3 Benefits and Challenges of Digital Payments
1.4 Payment Cards and Contactless Technologies
1.5Near Field Communication (NFC)
1.6 QR Code Payments
1.7 Peer-to-Peer (P2P) Payment Systems

Unit 2	**Security Foundations , Regulatory Framework and Compliance**	**6 Hours**

2.1 Encryption and Secure Sockets Layer (SSL)
2.2 Tokenization for Payment Security
2.3 Two-Factor Authentication (2FA)
2.4 Biometric Authentication in Digital Payments
2.5 Overview of Global Payment Regulations
2.6 Payment Card Industry Data Security Standard (PCI DSS)
2.7 General Data Protection Regulation (GDPR) and Privacy Concerns
2.8 Compliance in Cross-Border Transactions

Unit 3	Fraud Prevention and Detection	4 Hours
3.1 Common Types of Payment Fraud 3.2 Machine Learning in Fraud Detection 3.3 Behavioral Analytics for Fraud Prevention 3.4 Role of Digital Identity in Fraud Mitigation		
Unit 4	**Emerging Technologies in Digital Payments**	**4 Hours**
4.1 Blockchain and Cryptocurrencies 4.2 Central Bank Digital Currencies (CBDCs) 4.3 Internet of Things (IoT) in Payments 4.4 Contactless Wearables and Smart Devices		
Unit 5	**User Experience and Accessibility**	**4 Hours**
5.1 User-Centric Design in Digital Payment Applications 5.2 Accessibility and Inclusion in Digital Payments 5.3 Balancing Security and User Convenience 5.4 Human Factors in Cybersecurity Awareness		
Unit 6	**Future Trends and Challenges**	**4 Hours**
6.1 Evolving Landscape of Digital Payment Innovations 6.2 Cross-Border Payments and Global Interoperability 6.3 Ethical Considerations in Digital Payments 6.4 Addressing Cybersecurity Challenges in the Future of Payments		

Reference Books:

- Cyber Security and the Future of Digital Payments by Yeter Birik (Author)
- Digital Payments in India: Background, Trends and Opportunities by Jaspal Singh (Author)

MCS-511-MJP – Practical Based on MCS510MJ Digital Payments and Security		
Teaching Scheme 2 hours / week	**No. of Credits:2**	**Examination Scheme** CA :15 marks UA: 35 marks
Prerequisites: Should know the different modes of digital payment.		
Course Objectives: - To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.		
Course Outcomes: - Student will be able to :- • Develop a digital payment solution customized to the needs of their constituents.		
Practical List		

Assignment No 1

- How can multi-factor authentication enhance the security of digital payment transactions, and why is it important?

Assignment No 2

- What measures can be implemented to protect sensitive financial information during online transactions, considering the risk of data breaches?

Assignment No 3

- How do tokenization and encryption contribute to securing digital payment information, and what are their respective roles in the process?

Assignment No 4

- Explain the concept of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) in the context of online payments and its significance for secure communication.

Assignment No 5

- In the realm of digital payments, what challenges and security considerations should businesses address to ensure a safe and trustworthy payment environment for their customers?

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security))
Subject Code : MCS-512-MJ
Subject: Wireless Security

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites: Basic Knowledge of networking and encryption protocols

Course Objectives:-

- This skill oriented course equips the system Administrators with the skills required to protect & recover the computer systems & networks from various security threats

Course Outcomes:-Student will be able to:-

- Familiarize with the issues and technologies involved in designing a wireless system that is robust against various attacks.
- Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks

Course Contents

Unit 1	**Fundamentals of Wireless Security**	**4 Hours**

1.1 Overview of Wireless Networks
1.2 Importance of Wireless Security
1.3 Wireless Threat Landscape
1.4 Security Protocols in Wireless Communication

Unit 2	**Wireless Encryption Protocols**	**4 Hours**

2.1 WEP, WPA, and WPA2
2.2 WPA3 Security Enhancements
2.3 Enterprise Wireless Security (802.1X)
2.4 Key Management in Wireless Encryption

Unit 3	**Securing Wi-Fi Networks**	**4 Hours**

3.1 Wi-Fi Network Architecture
3.2 SSID Security Practices
3.3 MAC Filtering and Access Control
3.4 Wireless Intrusion Detection Systems (WIDS)

Unit 4	Advanced Wireless Threats and Countermeasures	6 Hours
4.1 Man-in-the-Middle (MitM) Attacks 4.2 Evil Twin and Rogue Access Points 4.3 Jamming and Deauthentication Attacks 4.4 Wireless Honeypots for Threat Detection		
Unit 5	**Mobile Device Security in Wireless Networks**	**3 Hours**
5.1 BYOD Policies and Security 5.2 Mobile Device Management (MDM) 5.3 Endpoint Security for Smartphones and Tablets 5.4 Secure Wi-Fi Connectivity for Mobile Devices		
Unit 6	**Wi-Fi Security Best Practices for Organizations**	**3 Hours**
6.1 Designing Secure Wi-Fi Networks 6.2 Security Policies and User Education 6.3 Periodic Security Audits and Assessments 6.4 Guest Wi-Fi Security Considerations		
Unit 7	**Wireless Security in the Internet of Things (IoT)**	**3 Hours**
7.1 IoT Devices and Connectivity 7.2 Security Challenges in IoT 7.3 Securing Wireless Communication in IoT 7.4 Integration with Wireless Access Controls		
Unit 8	**Emerging Trends in Wireless Security**	**3 Hours**
8.1 Wi-Fi 6 (802.11ax) and Security Implications 8.2 5G Networks and Security Challenges 8.3 Artificial Intelligence (AI) in Wireless Security 8.4 Future Directions and Innovations in Wireless Security		

Reference Books:

- Wireless Network Security: Second Edition by Wolfgang Osterhage (Author)
- Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise Paperback by J Minella (Author)
- Wireless and Mobile Device Security Paperback – Import, 14 April 2021 by Jim Doherty (Author)
- Wireless and Mobile Device Security by Jim Doherty
- Wireless Network Administration A Beginner's Guide. by Wale Soyinka.

MCS-513-MJP – Practical Based on MCS512MJ
Wireless Security

Teaching Scheme	**No. of Credits:2**	**Examination Scheme**
2 hours / week		CA :15 marks UA: 35 marks

Prerequisites: Should have basic knowledge about internetworking and network security

Course Objectives: -

- Implementation and management of network security
- Ethical implications of wireless networks

Course Outcomes: - Student will be able to :-

- Test and evaluate various wireless networks performance
- Apply and evaluate wireless network security techniques with consideration of ethical implications

Practical List

Assignment No 1

- How does WPA3 improve wireless security compared to its predecessors, and what are the key features that enhance protection?

Assignment No 2

- Can you explain the potential security risks associated with open Wi-Fi networks and suggest measures to secure them?

Assignment No 3

- What role does MAC address filtering play in wireless security, and are there any limitations or considerations to keep in mind when using this method?

Assignment No 4

- How can a rogue access point pose a security threat to a wireless network, and what steps can be taken to detect and mitigate such risks?

.

Assignment No 5

- Describe the importance of regularly updating firmware on wireless devices, such as routers and access points, in maintaining a secure wireless network environment.

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-514-MJ
Subject: IT Act.2000 in Cyber Space

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Knowledge of cyber laws

Course Objectives:-

- The course will provide knowledge regarding Issues of Internet Governance and International Organizations and their Roles to the students so that students do not face any difficulty while handling practical cases in future as an advocate.
- Knowledge of cyber Laws

Course Outcomes:-Student will be able to:-

- To understand Intellectual Property issues in IT Act
- To understand various aspects of cyber crimes

Course Contents

Unit 1	**Introduction to Information Technology Act 2000**	**3 Hours**

1.1 Background and Evolution
1.2 Objectives and Scope
1.3 Relevance in the Cyberspace

Unit 2	**Legal Framework for Electronic Transactions**	**4 Hours**

2.1 Digital Signatures and Authentication
2.2 Electronic Records and Recognition
2.3 Validity and Legality of Electronic Contracts
2.4 Legal Challenges and Case Studies

Unit 3	**Cybercrimes and Offenses**	**4 Hours**

3.1 Unauthorized Access and Hacking
3.2 Data Theft and Unauthorized Copying
3.3 Identity Theft and Impersonation
3.4 Cyber Stalking and Harassment

Unit 4	**Intermediary Liability and Responsibilities**	**4 Hours**

4.1 Definition of Intermediaries
4.2 Safe Harbor Provisions
4.3 Responsibilities of Internet Service Providers (ISPs)
4.4 Balancing Freedom and Regulation

Unit 5	**Investigation and Adjudication Processes**	**3 Hours**
5.1 Role of Cyber Cells and Law Enforcement 5.2 Search and Seizure in Cyberspace 5.3 Adjudication of Cybercrimes 5.4 Challenges in Digital Forensics and Evidence		
Unit 6	**Data Protection and Privacy**	**4 Hours**
6.1 Personal Data Protection Principles 6.2 Consent and Notice Requirements 6.3 Security Safeguards for Personal Data 6.4 Data Breach Reporting and Notification		
Unit 7	**Cyber Appellate Tribunal and Judicial Precedents**	**4 Hours**
7.1 Establishment and Functions of the Cyber Appellate Tribunal 7.2 Landmark Judgments and Precedents 7.3 Evolving Jurisprudence in Cyber Law 7.4 Contemporary Legal Challenges and Debates		
Unit 8	**Amendments and Future Prospects**	**4 Hours**
8.1 Amendments to the IT Act 2000 8.2 International Cooperation and Cybersecurity 8.3 Future Trends and Challenges in Cyberspace Regulation 8.4 Global Alignment and Harmonization of Cyber Laws		
Reference Books:		
• (2022 edition) The Information Technology Act, 2000 [Universal's-New Delhi] Paperback – 1 January 2021 by Lexis (Author) • Law of Information Technology and Cyberspace Paperback – 1 January 2019 by Dr. N. Maheshwara Swamy (Author)		

MCS-515-MJP: Practical Based on MCS 514MJ
IT Act.2000

Teaching Scheme	**No. of Credits:2**	**Examination Scheme**
2 hours / week		CA :15 marks UA: 35 marks

Prerequisites:

- Basic Knowledge of cyber laws

Course Objectives:-

- The course will provide knowledge regarding Issues of Internet Governance and International Organizations and their Roles to the students so that students do not face any difficulty while handling practical cases in future as an advocate.
- Knowledge of cyber Laws

Course Outcomes:-Student will be able to:-

- To understand Intellectual Property issues in IT Act
- To understand various aspects of cyber crimes

Practical List

Assignment 1
How does the Information Technology Act of 2000 address issues related to electronic authentication and digital signatures in cyberspace?

Assignment 2
Can you explain the provisions within the IT Act 2000 that pertain to the unauthorized access and hacking of computer systems and networks?

Assignment 3
What role does the IT Act play in regulating and penalizing cybercrimes such as data breaches, identity theft, and online fraud?

Assignment 4
How does the IT Act address issues of intermediary liability and the responsibilities of online service providers for content hosted on their platforms?

Assignment 5
Can you provide an overview of the legal framework outlined in the IT Act regarding the investigation and prosecution of cyber offenses in India?

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-531-RM
Subject: Research Methodology

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Ability to think critically about a topic and the sources necessary to study and limit that topic.

Course Objectives:-

- Research Methodology course are designed to equip students with the necessary knowledge, skills, and understanding of various research techniques and methodologies.
- Students should be familiar with various data collection techniques, such as surveys, interviews, observations, and experiments, and understand their strengths and limitations.
- Students should be aware of ethical considerations in research, including issues related to participant consent, privacy, confidentiality, and avoiding plagiarism.
- Its aim is to enable students to conduct research effectively, critically evaluate existing research, and contribute to the advancement of knowledge in their respective fields.

Course Outcomes:-Student will be able to:-

CO 1. Understand of the fundamental concepts of research, including the research process,research questions, hypotheses, and variables.

CO 2. Conduct a comprehensive literature review to identify relevant studies, synthesize existing knowledge, and identify research gaps.

CO 3. Identify research problems, formulate research questions, and design appropriate methodologies to address these problems

CO 4. Identify and select appropriate research designs, such as experimental, observational,survey, qualitative, or mixed-methods, based on the research objectives.

Course Contents

Unit 1	**Introduction to Research Methodology**	**3 Hours**

1.1. Meaning of Research
1.2. Objectives of Research
Types of Research
1.3. Research Approaches
1.4. Significance of Research
1.5. Researcher and Characteristics of Researcher
1.6. Research Ethics and Integrity
1.7. Plagiarism and types of plagiarism
1.8. Introduction to Plagiarism check tools
1.9. Research Methods versus Methodology

Unit 2	Literature Review and Formulation of Research Problems	6 Hours

1.1. Research Process
1.2. Reviewing the literature: purpose of a literature review
1.3. Literature resources
1.4. The Internet and a literature review
1.5. The Internet and research strategies and methods
1.6. Conducting and Evaluating literature reviews
1.7. Formulation of research problem
    1.7.1. What is a Research Problem?
    1.7.2. Selecting the Problem
    1.7.3. Necessity of Defining the Problem
2. Technique Involved in Defining a Problem

Unit 3	Research Design	8 Hours

1.1. Need for Research Design
1.2. Meaning & Features of a Good Design
1.3. Important Concepts Relating to Research Design
1.4. Different Research Designs/Methods
    1.4.1. Pure and Applied Research
    1.4.2. Exploratory or Formulative Research
    1.4.3. Descriptive Research
    1.4.4. Diagnostic Research
    1.4.5. Evaluation Studies
    1.4.6. Action Research
    1.4.7. Experimental Research
    1.4.8. Analytical Study or Statistical Method
    1.4.9. Historical Research
    1.4.10. Surveys
    1.4.11. Case Study
2. Field Studies

Unit 4	Hypothesis and Sampling	4 Hours

1.1. What is Hypothesis?
1.2. Nature & Characteristics of Hypothesis
1.3. Significance of Hypothesis
2. Types of Hypothesis
    2.1. Sources of Hypothesis
    2.2. Characteristics of Good Hypothesis
    2.3. What is sampling?
    2.4. Aims of Sampling
    2.5. Characteristics of Good Sample
    2.6. Basis of Sampling
    2.7. Merits and demerits of Sampling

2.8. Sampling Techniques or Methods
2.9. Probability Sampling Methods
2.10. Non-Probability Sampling Methods
3. Sample Design and Choice of Sampling Technique

Unit 5	Data Collection, Processing and Analysis of Data	3 Hours

1.1. Collection of Primary Data
1.2. Method of data Collections - Observation, Interview, Questionnaires andSchedules etc.
1.3. Difference between Questionnaires and Schedules
1.4. Collection of Secondary Data
1.5. Selection of Appropriate Method for Data Collection
1.6. Case Study Method
1.7. Processing Operations and Some Problems in Processing
1.8. Elements/Types of Data Analysis
1.9. Statistics in Research
1.10. Measures of Central Tendency, Dispersion, Asymmetry (Skewness)
1.11. Measures of Relationship - Chi-Square, t-test, ANNOVA(f-test),Z-test
1.12. Simple Regression Analysis, and Multiple Correlation and Regression
1.13. Partial Correlation and Association in Case of Attributes
2. Quantitative and Qualitative Data Analysis Tools

Unit 6	Interpretation and Report Writing	4 Hours

1.1. Meaning of Interpretation, Why Interpretation?
1.2. Technique of Interpretation
1.3. Precaution in Interpretation
1.4. Significance of Report Writing
1.5. Different Steps in Writing Report
1.6. Layout of the Research Report
1.7. Types of Reports (Research Proposal/Synopsis, Research Paper, and Thesis)
1.8. Oral Presentation
1.9. Mechanics of Writing a Research Report
2. Precautions for Writing Research Reports

Unit 7	Publication Ethics and Open Access Publishing	4 Hours

1.1. Publication ethics: definition, introduction and importance
1.2. Best practices/standards setting initiatives and guidelines: COPE, WAME, etc.
1.3. Conflicts of interest
2. Publication misconduct: definition, concept, problems that lead to unethicalbehaviour and vice versa, types
2.1. Violation of publication ethics, authorship and contributor ship
2.2. Identification of publication misconduct, complaints and appeals

2.3. Predatory publishers and journal
2.4. Open access publications and initiatives
2.5. SHERPA/RoMEO online resource to check publisher copyright & self-archivingpolicies
2.6. Software tool to identify predatory publications
2.7. Journal finder/ journal suggestion tools viz. JANE, Elsevier Journal Finder,Springer Journal Suggester, etc.

3. E-Resources for research: Google Scholar, Shodh Ganaga, Shodh Gangotri

Reference Books:

1. Researching Information Systems and Computing by Briony J Oates, SAGE SOUTH ASIA Ed
2. Research Methodology: A Step-by-Step Guide for Beginners, Kumar, Pearson Education.
3. Research Methodology Methods and Techniques, Kothari, C. R., Wiley Eastern Ltd.
4. The Research Methods Knowledge Base, by William M. K. Trochim, James P. Donnelly
5. Introducing Research Methodology: A Beginner‟s Guide to Doing a Research Project, Uwe Flick

Semester II

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-551-MJ
Subject: Mobile Application and Services

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Knowledge of networking and applications

Course Objectives:-

- Creating robust mobile applications and learn how to integrate them with other services
- Creating intuitive, reliable mobile apps using the android services and components

Course Outcomes:-Student will be able to:-

- Explain and use key Android programming concepts
- Understand both the basic and advanced concepts Android Programming Platforms

Course Contents

Unit 1	**Introduction to Mobile Applications Services and Development**	**4 Hours**

1.1 Evolution of Mobile Technology
1.2 Mobile Operating Systems
1.3 Significance of Mobile Applications and Services
1.4 Trends and Innovations in Mobile Technology
1.5 Mobile App Architecture
1.6 Native vs. Hybrid vs. Web Apps
1.7 Cross-Platform Development Frameworks
1.8 Mobile App Lifecycle and Deployment

Unit 2	**Security in Mobile Applications**	**4 Hours**

2.1 Secure Coding Practices
2.2 Data Encryption and Storage
2.3 User Authentication and Authorization
2.4 Mobile App Penetration Testing

Unit 3	Monetization and Business Models for Mobile Apps	5 Hours
3.1 In-App Purchases and Freemium Models 3.2 Ad-Based Revenue Models 3.3 Subscription Services 3.4 Challenges and Strategies in App Monetization		
Unit 4	**User Experience (UX) and Interface Design**	**4 Hours**
4.1 Principles of Mobile UX Design 4.2 Responsive Design for Various Devices 4.3 Accessibility and Inclusivity in Mobile UI/UX 4.4 Usability Testing for Mobile Applications		
Unit 5	**Mobile App Analytics and Performance Optimization**	**4 Hours**
5.1 Importance of Analytics in Mobile Apps 5.2 Key Performance Indicators (KPIs) for Mobile Apps 5.3 A/B Testing and User Feedback 5.4 Strategies for Optimizing App Performance		
Unit 6	**Mobile Services and Integration**	**4 Hours**
6.1 Cloud Services and Mobile Integration 6.2 Location-Based Services (LBS) 6.3 Augmented Reality (AR) and Virtual Reality (VR) 6.4 Mobile Payments and NFC Integration		
Unit 7	**Emerging Technologies in Mobile Applications**	**5 Hours**
7.1 Internet of Things (IoT) and Mobile Integration 7.2 Artificial Intelligence (AI) in Mobile Apps 7.3 Edge Computing for Mobile Services 7.4 Wearable Technology and Mobile Connectivity		
Reference Books:		
• Mobile Communications Paperback – 4 March 2003 by Dr Jochen Schiller (Author) • Mobile Communications, 2e 2nd Edition, Kindle Edition by Jochen Schiller (Author)		

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-552-MJ
Subject: Incident Handling

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- An understanding of internet services and protocols
- Experience with various types of computer security attacks, response strategies, incident handling tools

Course Objectives:-

- Have an understanding of the fundamentals of computer forensics and forensic readiness
- Apply the right techniques to different types of cyber security incidents in a systematic manner (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents)
- Master all incident handling and response best practices, standards, cyber security frameworks, laws, acts, and regulations

Course Outcomes:-Student will be able to:-

- The student has general knowledge of planning for incident response readiness and managing the operational aspects of the incident response team.
- The student understands cyber incident response and its components.
- The student has a good overview of known frameworks and tools for incident response

Course Contents

Unit 1	**Introduction to Incident Handling**	**4 Hours**

1.1 Definition and Importance
1.2 Incident Handling Lifecycle
1.3 Incident Categories and Classifications
1.4 Legal and Regulatory Considerations in Incident Handling

Unit 2	**Incident Detection and Reporting**	**4 Hours**

2.1 Proactive vs. Reactive Detection
2.2 Security Information and Event Management (SIEM)
2.3 Incident Reporting Procedures
2.4 Automation in Incident Detection

Unit 3	Incident Triage and Initial Response	4 Hours
3.1 Incident Triage Process 3.2 Prioritization and Categorization 3.3 First Responder Actions 3.4 Communication Protocols during Initial Response		
Unit 4	**Incident Investigation and Analysis**	**4 Hours**
4.1 Digital Forensics in Incident Handling 4.2 Evidence Collection and Preservation 4.3 Analysis of System Logs and Artifacts 4.4 Collaborative Investigation Techniques		
Unit 5	**Incident Containment , Eradication Recovery and System Restoration**	**6 Hours**
5.1 Containment Strategies 5.2 Isolation and Segmentation 5.3 Eradication Techniques 5.4 Validation of Containment and Eradication 6.1 Data Recovery and Restoration 5.5 System Rebuilding and Patching 5.6 Communication with Stakeholders 5.7 Lessons Learned and Documentation		
Unit 6	**Communication and Coordination**	**4 Hours**
6.1 Internal Communication Protocols 6.2 External Communication with Stakeholders 6.3 Coordination with Incident Response Teams 6.4 Media and Public Relations in Incident Handling		
Unit 7	**Post-Incident Analysis and Improvement**	**4 Hours**
7.1 Post-Incident Review Meetings 7.2 Incident Reporting and Documentation 7.3 Continuous Improvement in Incident Handling 7.4 Incorporating Lessons Learned in Security Policies		
Reference Books:		

- Incident Handling and Response: A Holistic Approach for an efficient Security Incident Management. Kindle Edition by Jithin Alex (Author)
- Intelligence–Driven Incident Response: Outwitting the Adversary Paperback – Import, 5 September 2017 by Scott Roberts (Author), Rebekah Brown (Author)

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-553-MJ
Subject: Cyber Security Architecture

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Basic Knowledge of cyber Security

Course Objectives:-

- To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.
- To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.

Course Outcomes:-Student will be able to:-

- Be able to use cyber security, information assurance, and cyber/computer forensics software/tools.
- Design and develop a security architecture for an organization.
- Design operational and strategic cyber security strategies and policies

Course Contents

Unit 1	**Foundations of Cybersecurity Architecture**	**4 Hours**

1.1 Introduction to Cybersecurity Architecture
1.2 Importance of Robust Security Architecture
1.3 Key Principles and Objectives
1.4 Relationship with Enterprise Architecture

Unit 2	Network Security Architecture	**3 Hours**

2.1 Perimeter Security and Network Segmentation
2.2 Firewalls, Routers, and Intrusion Detection Systems (IDS)
2.3 Virtual Private Networks (VPNs) and Secure Sockets Layer (SSL)
2.4 Defense-in-Depth Strategies

Unit 3	Identity and Access Management (IAM) Architecture	**3 Hours**

3.1 Role of IAM in Cybersecurity
3.2 Authentication and Authorization Mechanisms
3.3 Single Sign-On (SSO) Solutions
3.4 Identity Federation and Lifecycle Management

Unit 4	**Endpoint Security Architecture**	**4 Hours**
4.1 Endpoint Protection Platforms (EPP) 4.2 Antivirus and Anti-Malware Solutions 4.3 Device Encryption and Data Loss Prevention (DLP) 4.4 Mobile Device Management (MDM) Integration		
Unit 5	Cloud Security Architecture	**5 Hours**
5.1 Cloud Security Fundamentals 5.2 Shared Responsibility Model 5.3 Identity and Access Management in Cloud 5.4 Data Encryption and Key Management		
Unit 6	Application Security Architecture	**4 Hours**
6.1 Secure Software Development Life Cycle (SDLC) 6.2 Web Application Firewalls (WAF) 6.3 Code Analysis and Penetration Testing 6.4 API Security Considerations		
Unit 7	Incident Response and Security Operations Center (SOC) Architecture	**4 Hours**
7.1 Establishing an Incident Response Framework 7.2 Security Information and Event Management (SIEM) 7.3 Threat Intelligence Integration 7.4 Collaboration with External Incident Response Teams		
Unit 8	Incident Response and Security Operations Center (SOC) Architecture	**3 Hours**
8.1 Zero Trust Architecture 8.2 Artificial Intelligence and Machine Learning Integration 8.3 Continuous Monitoring and Adaptive Security 8.4 Blockchain and Decentralized Security Architectures		

Reference Books:

- Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects Paperback – Import, 20 November 2020 by Ed Moyle (Author), Diana Kelley (Author)
- Secrets of a Cyber Security Architect Hardcover – 5 December 2019 by Brook S. E. Schoenfield (Author)
- Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects Paperback – Import, 20 November 2020

MCS-554-MJP: Practical Based on MCS 551MJ Mobile Application and Services		
Teaching Scheme 2 hours / week	**No. of Credits:2**	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:

Basic Knowledge about Mobile Applications.

Course Objectives: -

- Create a seamless user interface that works with different mobile screens
- To help students to gain a basic understanding of Android application development

Course Outcomes: - Student will be able to :-

- Program mobile applications for the Android operating system that use basic and advanced phone features.
- Identify various concepts of mobile programming that make it unique from programming for other platforms.

Practical List

Assignment 1

How can mobile application developers implement secure coding practices to mitigate common security risks such as injection attacks and data leaks?

Assignment 2

What measures should be taken to ensure the privacy of users when designing and developing mobile applications that collect personal information?

Assignment 3

How does mobile device management (MDM) contribute to the security of enterprise mobile applications and services?

Assignment 4

Explain the importance of regular security updates for mobile applications and the potential risks associated with neglecting these updates.

Assignment 5

In the context of mobile services, what strategies can be employed to protect against mobile malware, phishing attacks, and other threats targeting users on mobile platforms?

MCS-555-MJP: Practical Based on MCS 552MJ
Incident Handling

Teaching Scheme	**No. of Credits:2**	**Examination Scheme**
2 hours / week		CA :15 marks UA: 35 marks

Prerequisites:
1. Should have basic knowledge of incident Handling regarding Cyber Security

- **Course Objectives: -** Decode the various steps involved in planning incident handling and response program (Planning, Recording and Assignment, Triage, Notification, Containment, Evidence Gathering and Forensic Analysis, Eradication, Recovery, and Post-Incident Activities)
- Apply the right techniques to different types of cyber security incidents in a systematic manner (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents)

Course Outcomes: - Student will be able to :-

- Investigate incidents by executing the system event log analysis.
- perform basic network forensic analysis.

Practical List

Assignment 1
What are the key steps involved in an effective incident handling process, from detection to resolution?

Assignment 2
How do you prioritize incidents during an incident response, and what factors influence your decision-making?

Assignment 3
Can you explain the role of a Computer Security Incident Response Team (CSIRT) and its responsibilities in handling and mitigating security incidents?

Assignment 4
In the aftermath of a security incident, what measures should be taken to conduct a thorough post-incident analysis and improve future incident response capabilities?

Assignment 5
How do you communicate with stakeholders, both internal and external, during different stages of incident handling to ensure a coordinated and transparent response?

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-560-MJ
Subject: Dark Web & Cyber Warfare

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites: Knowledge of Networking and VPN secuirty

Course Objectives:-

- To gain knowledge on the working of Dark Web
- To understand the operational procedures of cyber war and to have clarity on defense mechanism
- To identify the security aspects of dark net.

Course Outcomes:-Student will be able to:-

- Able to work in Law enforcement for cybercrime investigation w.r.t to dark web and warfare
- Able to understand the deep / dark web attacks
- Able to use the deep web operating system and apply the security measures

Course Contents

Unit 1	**Introduction to the Dark Web**	**4 Hours**

1.1 Definition and Characteristics
1.2 Technologies Facilitating Dark Web Access
1.3 Key Components: Tor, I2P, and Freenet
1.4 Legal and Ethical Considerations

Unit 2	**Dark Web Marketplaces**	**4 Hours**

2.1 Overview of Underground Marketplaces
2.2 Illicit Goods and Services
2.3 Cryptocurrencies and Transactions
2.4 Challenges in Law Enforcement

Unit 3	Cybercrime on the Dark Web	5 Hours
3.1 Types of Cybercrime Activities 3.2 Hacking Services and Tools 3.3 Stolen Data Trade 3.4 Advanced Persistent Threats (APTs) for Sale		
Unit 4	**Cyber Warfare Fundamentals**	**4 Hours**
4.1 Definition and Objectives 4.2 State Sponsored Cyber Attacks 4.3 Non State Actors in Cyber Warfare 4.4 The Role of Hacktivism		
Unit 5	**Techniques and Tactics in Cyber Warfare**	**4 Hours**
5.1 Malware in Cyber Warfare 5.2 Denial of Service (DoS) and Distributed Denial of Service (DDoS) 5.3 Spear Phishing and Social Engineering 5.4 Advanced Persistent Threats (APTs)		
Unit 6	**Attribution Challenges in Cyber Warfare**	**5 Hours**
6.1 The Problem of Identifying Cyber Attackers 6.2 False Flag Operations 6.3 Nation State Tactics for Anonymity 6.4 International Collaboration in Attribution		
Unit 7	**Countermeasures and Cybersecurity in Dark Web and Cyber Warfare**	**4 Hours**
7.1 Dark Web Monitoring and Law Enforcement 7.2 Cybersecurity Strategies for Organizations 7.3 International Agreements and Cyber Norms 7.4 Ethical Hacking and Offensive Cyber Operations		

Reference Books:

- Threat Hunting, Hacking, and Intrusion Detection - (SCADA, Dark Web, and APTs): Cyber Secrets 1 [Print Replica] Kindle Edition by Jeremy Martin (Author), Richard Medlin (Author), Nitin Sharma (Author), James Ma (Author), & 2 More Format: Kindle Edition
- Understanding Cyber Warfare: Politics, Policy and Strategy Paperback – 6 December 2018 by Christopher Whyte (Author), Brian Mazanec (Author)
- The Dark Web: Breakthroughs in Research and Practice (Critical Explorations) Hardcover – Import, 30 July 2017 by Information Resources Management Association (Author)

MCS-561-MJP: Practical Based on MCS 560MJ Dark Web and Cyber Warfare		
Teaching Scheme 2 hours / week	**No. of Credits:2**	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:
Basic Knowledge of networking

Course Objectives: -

- To understand the dark web security trends and measures in mobile and wireless devices.
- To understand different tools and methods used in Dark Web.

Course Outcomes: - Student will be able to :-

Understand different attacks in Dark Web.
Expose to tools and methods used in Dark Web.

Practical List

Assignment 1
How does the dark web contribute to cybercrime, and what challenges does it pose for law enforcement and cybersecurity professionals?

Assignment 2
Can you explain the role of cryptocurrencies in facilitating transactions on the dark web and the implications for tracking illegal activities?

Assignment 3
In the context of cyber warfare, what are the potential threats posed by state-sponsored hacking groups, and how do they differ from conventional cybercriminal activities?

Assignment 4
How can nations strengthen their cybersecurity posture to defend against cyber warfare attacks, considering the evolving tactics and techniques used by nation-state actors?

Assignment 5
Describe the ethical and legal considerations associated with offensive cybersecurity operations in the realm of cyber warfare, including the use of tools like malware and advanced persistent threats (APTs).

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-562-MJ
Subject: DevSecOps

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Students Should have a baseline knowledge and understanding of common DevOps definitions and principles

Course Objectives:-

- Contrast the options used to build a DevSecOps infrastructure through Platform as a Service, Server-less construction, and event-driven mediums.
- Identify future trends that may affect DevSecOps
- Distinguish between the technical elements used across DevSecOps practices

Course Outcomes:-Student will be able to:-

- Students will be able to Explain goals for a DevSecOps toolchain approach

Course Contents

Unit 1	Introduction to DevSecOps	**4 Hours**

1.1 Evolution of DevSecOps
1.2 Key Principles and Objectives
1.3 Integration with DevOps
1.4 Benefits of DevSecOps Adoption

Unit 2	Shifting Left in DevSecOps	**3 Hours**

2.1 Early Integration of Security in SDLC
2.2 Code Analysis and Automated Testing
2.3 Threat Modeling and Risk Assessment
2.4 Collaboration between Development and Security Teams

Unit 3	Automation in DevSecOps	**4 Hours**

3.1 Continuous Integration and Continuous Deployment (CI/CD)
3.2 Automated Security Testing
3.3 Infrastructure as Code (IaC)
3.4 Configuration Management for Security

Unit 4	Secure Coding Practices	**4 Hours**
4.1 Coding Standards and Guidelines 4.2 Common Vulnerabilities and Mitigations 4.3 Code Reviews and Security Audits 4.4 Developer Training and Awareness		
Unit 5	Container Security in DevSecOps	**4 Hours**
5.1 Docker and Containerization Security 5.2 Orchestration Platforms (e.g., Kubernetes) 5.3 Image Scanning and Vulnerability Management 5.4 Securing Microservices Architectures		
Unit 6	Identity and Access Management in DevSecOps	**3 Hours**
6.1 RoleBased Access Control (RBAC) 6.2 Least Privilege Principle 6.3 Single SignOn (SSO) Integration 6.4 Managing Credentials and Secrets		
Unit 7	Compliance and Governance in DevSecOps	**4 Hours**
7.1 Regulatory Compliance Considerations 7.2 Audit Trails and Monitoring 7.3 Documentation and Reporting 7.4 Aligning DevSecOps with Industry Standards		
Unit 8	DevSecOps Best Practices and Continuous Improvement	**4 Hours**
8.1 Performance Metrics and Key Performance Indicators (KPIs) 8.2 Incident Response in DevSecOps 8.3 Feedback Loops and Iterative Improvement 8.4 Cultural Shifts and Organizational Adoption		
Reference Books:		
• DevSecOps: A leader's guide to producing secure software without compromising flow, feedback and continuous improvement Paperback – 10 December 2020 by Glenn Wilson (Author) • Implementing DevSecOps with Docker and Kubernetes: An Experiential Guide to Operate in the DevOps Environment for Securing and Monitoring Container Applications Paperback – 21 February 2022 by José Manuel Ortega Candel (Author)		

MCS-563-MJP: Practical Based on MCS 562MJ DevSecOps		
Teaching Scheme 2 hours / week	**No. of Credits:2**	**Examination Scheme** CA :15 marks UA: 35 marks
Prerequisites: Should have Practice to design and implement security solutions		
Course Objectives: - • Develop cyber security strategies and policies • Understand principles of web security and to guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.		
Course Outcomes: - Student will be able to :- • The purpose, benefits, concepts and vocabulary of DevSecOps**.** • Business-driven security strategies and Best Practices**.**		
Practical List		
Assignment 1 What is DevSecOps, and how does it integrate security practices into the DevOps pipeline? Assignment 2 Explain the concept of "shifting left" in DevSecOps and its significance in addressing security concerns earlier in the software development life cycle. Assignment 3 How can automation be leveraged in DevSecOps to enhance security processes, such as continuous integration, continuous delivery, and continuous testing? Assignment 4 What are the key benefits of implementing a DevSecOps culture in terms of improving collaboration between development, operations, and security teams? Assignment 5 Describe the role of container security and orchestration tools in ensuring the security of applications deployed in a DevSecOps environment.		

Savitribai Phule Pune University
F.Y.M.Sc.(Cyber Security)
Subject Code : MCS-564-MJ
Subject: Tools & Technology for Cyber Security

Teaching Scheme	No. of Credits	Examination Scheme
2 hours / week	2	CE:15 marks EE:35marks

Prerequisites:

- Students should have basic knowledge about Cyber Security Tool and Technology

Course Objectives:-

- Understand principles of web security and to guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.
- Understand key terms and concepts in Cryptography, Governance and Compliance
- Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization

Course Outcomes:-Student will be able to:-

- Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators.
- Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools

Course Contents

Unit 1	Network Security Tools	**3 Hours**

1.1 Firewall Technologies
1.2 Intrusion Detection Systems (IDS)
1.3 Intrusion Prevention Systems (IPS)
1.4 Network Scanners and Vulnerability Assessment Tools

Unit 2	Endpoint Security Solutions	**4 Hours**

2.1 Antivirus and AntiMalware Software
2.2 Endpoint Detection and Response (EDR)
2.3 Mobile Device Management (MDM) Tools
2.4 Data Loss Prevention (DLP) Solutions

Unit 3	Identity and Access Management (IAM) Tools	**4 Hours**

3.1 Single SignOn (SSO) Solutions
3.2 MultiFactor Authentication (MFA)
3.3 Privileged Access Management (PAM)
3.4 Identity Governance and Administration (IGA) Tools

Unit 4	Encryption Tools	**4 Hours**
4.1 Full Disk Encryption 4.2 File and Folder Encryption 4.3 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) 4.4 Public Key Infrastructure (PKI) Solutions		
Unit 5	Security Information and Event Management (SIEM) Systems	**4 Hours**
5.1 Log Management and Analysis 5.2 Correlation and Alerting 5.3 Incident Response Automation 5.4 Threat Intelligence Integration		
Unit 6	Incident Response Tools	**4 Hours**
6.1 Forensic Analysis Tools 6.2 Memory Forensics Tools 6.3 Network Forensics Solutions 6.4 Automated Incident Response Platforms		
Unit 7	Web Application Security Tools	**4 Hours**
7.1 Web Application Firewalls (WAF) 7.2 Static Application Security Testing (SAST) 7.3 Dynamic Application Security Testing (DAST) 7.4 Runtime Application Self Protection (RASP)		
Unit 8	Emerging Technologies in Cybersecurity Tools	**3 Hours**
8.1 Artificial Intelligence (AI) and Machine Learning (ML) in Security 8.2 Deception Technologies 8.3 Cloud Security Tools 8.4 Container Security Solutions		
Reference Books:		
• Exploring the Foundations and Essential Tools/Software of Cyber Security Kindle Edition by Cyber AI Lawyer Astral Alchemist (Author)		

MCS-565-MJP: Practical Based on MCS 564MJ Tools & technology for Cyber Security		
Teaching Scheme 2 hours / week	**No. of Credits:2**	**Examination Scheme** CA :15 marks UA: 35 marks

Prerequisites:

1. Fundamentals of Cyber Security

Course Objectives: -

- Make familiar with basic and advanced tools to provide sufficient information to respond appropriately to a network

Course Outcomes: - Student will be able to :-

- Understand the types of malware, including rootkits, Trojans, and viruses.
- Understand the different tools

Practical List

Assignment 1
Which network security tools are commonly used to monitor and protect against potential cyber threats?

Assignment 2
Can you name a few popular vulnerability scanning tools and explain their role in identifying weaknesses in a system's security?

Assignment 3
How do endpoint protection platforms contribute to overall cybersecurity, and what features should be considered when selecting such tools?

Assignment 4
What role does a Security Information and Event Management (SIEM) system play in aggregating and analyzing security data for proactive threat detection?

Assignment 5
Can you provide examples of encryption tools used to secure data in transit and at rest, and how do they enhance overall cybersecurity?