GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATONS

Programme	M.Sc.IT(Cyber Security)	Branch/Spec.	DCS
Semester	I	Version	1.0.0.0
Effective from Academic Year	2018-19	Effective for the batch Admitted in	July 2018
Subject code	P71A1DSF	Subject Name	Digital Security and Forensic Fundamental

Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	-	4	-	07	Theory	40	60	100
Hours	3	-	4	-	07	Practical	20	30	50

Pre-requisites:

Required Knowledge of any Operating System, Networking and Digital Security Issues

Learning Outcome:

-Able to identify security risks and take preventive steps
-Investigate cybercrime and collect evidences
-Able to use knowledge of forensic tools and software

Theory syllabus

Unit	Content	Hrs
1	**Digital Securities** Introduction, Types of Attacks, Digital Privacy, Online Tracking, Privacy Laws, Types of Computer Security risks (Malware, Hacking, Pharming, Phishing, Ransomware, Adware and Spyware, Trojan, Virus, Worms, WIFI Eavesdropping, Scareware, Distributed Denial-Of-Service Attack, Rootkits, Juice Jacking), Antivirus and Other Security solution, Password, Secure online browsing, Email Security, Social Engineering, Secure WIFI settings, Track yourself online, Cloud storage security, IOT security, Physical Security Threads	8
2	**Online Anonymity** Anonymous Networks, Tor Network, I2P Network, Freenet, Darknet, Anonymous OS – Tails, Secure File Sharing, VPN, Proxy Server, Connection Leak Testing, Secure Search Engine, Web Browser Privacy Configuration, Anonymous Payment	6
3	**Cryptography and Secure Communication** The Difference Between Encryption and Cryptography, Cryptographic Functions, Cryptographic Types, Digital Signature, The Difference Between Digital Signatures and Electronic Signatures, Cryptographic Systems Trust Models, Create a Cryptographic Key Pair Using Gpg4win/gpg4usb, Disk Encryption Using Windows BitLocker, Disk Encryption Using Open Source Tools, Multitask Encryption Tools, Attacking Cryptographic Systems, Countermeasures Against Cryptography Attacks, Securing Data in Transit, Cloud Storage Encryption, Encrypt DNS Traffic and Email communication, Secure IM and video calls	10

4	**Cyber Crime Issues and Investigation** Unauthorized Access, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses, Investigation Tools, e-Discovery, EDRM Model, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking	10
5	**Digital Forensics** Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, WIFI Security (War-driving), Network Forensics, Mobile Forensics, Cloud Forensics.	10
Practical content		
List of programs specified by the subject teacher based on above mentioned topics		
Text Books		
1	Digital Privacy and Security Using Windows: A Practical Guide By Nihad Hassan, Rami Hijazi, Apress	
Reference Books		
1	Digital Forensics, DSCI - Nasscom, 2012.	
2	Cyber Crime Investigation, DSCI - Nasscom, 2013.	
	Question Paper Scheme: **Note for Examiner** Q-1 must be common from any topics from syllabus. Q-2 and onwards must be from specific topics and internal choice or option can be given **Paper Structure** **Section - 1** Q-1 (Attempt any Five Out of Seven: each question must be 6 marks) --- 30 **Section - 2** Questions must be covered all possible section. Q-2 (Must be From topics: Digital Security and Online Anonymity (12 marks)) Q-3 (Must be From topics: Cryptography and Secure Communication and Cyber Crime Issues and Investigation (12 marks)) Q-4 (Must be From topic: Digital Forensics (6 marks))	

Note:

Version 1.0.0.0 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme, Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision)

L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work CE= Continuous Evaluation, SEE= Semester End Examination

GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATONS

Programme	M.Sc. IT(CYBER SECURITY)				Branch/Spec.	Computer Application		
Semester	I				Version	1.0.0.0		
Effective from Academic Year			2018-19		Effective for the batch Admitted in		July 2018	
Subject code	P71A2ATD		Subject Name		APPLICATION THREAT DETECTION			
Teaching scheme					Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	-	2	-	05	Theory	40	60	100
Hours	3	-	4	-	07	Practical	20	30	50

Pre-requisites:

Basic Knowledge of web application, Database and SQL is essential, Hands of experience of Linux OS.

Learning Outcome:

This course provides students basic knowledge and skills in detecting and defending threat to web Application. Upon Completion of the expected to have met the following course objectives

- Can detect threats to any web app.
- Able to perform various Input Injection Attacks.
- Able to provide countermeasures against various input injection attacks.

Theory syllabus

Unit	Content	Hrs
1	**Hacking Web Apps and Profiling.** Web Application Hacking: GUI web Hacking, URI Hacking, Methods Headers and Body, Resources. The Web Client and HTML, Other Protocols, How & Why Web Apps attack. **Infrastructure Profiling:** Footprinting and Scanning, Basic Banner Grabbing, Advanced HTTP Fingerprinting, Infrastructure Intermediaries. **Application Profiling**: Manual Inspection, Search Tools for Profiling, Automated Web Crawling, General Countermeasures.	09
2	**Bypassing and Attacking Web Authentication** **Web Authentication Threats:** Username/password Threats, Password Guessing and its Countermeasures, Eavesdropping attacks and its Countermeasures, Forms-based Authentication attacks and its countermeasures. Stronger web Authentication, Web Authentication Services. **Bypassing Authentication:** Token Replay, Cross-site Request Forgery, Identity Management.	08
3	**Penetration Testing and Input Injection Attacks.** Where to find Attack vectors, Common Input Injection Attacks: Buffer Overflow, Canonicalization and its countermeasures, Advanced Directory Traversal, Navigating Without Directory Listing, HTML Injection: XSS,	10

	Embedded scripts, Cookies and Predefined Headers, Counter countermeasures. **SQL Injection:** SUB Queries, UNION, Sql Injection countermeasures, XPATH Injection and its countermeasures, LDAP Injection.	
4	**Metasploit** **Basics of Penetration Testing:** The Phase of PTES, Types of Penetration Tests. **Metasploit:** Introduction, **Metasploit Basics:** Terminology, Metasploit Interfaces, Metasploit Utilities. **Intelligence Gathering:** Passive Information Gathering, Active Information Gathering, Target Scanning. **Vulnerability Scanning:** Basic Vulnerability Scan, Scanning with scanning tools, Using Scan Results for Autopwning.	10
5	**Attacking Users** Defacing Content, Capturing User Input: Using Focus Event, Using Keyboard Events, Using Mouse and Pointer Events, Using Form Events, Social Engineering: Using TabNabbing, Abusing UI Expectations: Using Fake Login Prompts, Pretty Theft, Gmail Phishing.	08
Practical content		
List of programs specified by the subject teacher based on above mentioned topics		
Text Books		
1	Hacking Exposed Web Application, 3rd Edition by Joel Scambray, Vincent Liu, Caleb Sima	
2	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto Wiley Publication	
3	Metasploit - The Penetration Tester's Guide by David Kennedy , Jim O'gorman , Devon Kearns and Mati Aharoni – No Starch Press Publication	
Reference Books		
1	The Browser Hacker's Handbook by Wade Alcorn, Christian Frichot and Michele Orru – Wiley Publication	
2	Web Penetration Testing with Kali Linux by Joseph Muniz, Aamir Lakhan – Packt Publication	
Question Paper Scheme:		
	Note for Examiner Q-1 must be common from any topics from syllabus. Q-2 and onwards must be from specific topics and internal choice or option can be given **Paper Structure** **Section :1** Q-1 (Attempt any Five Out of Seven: each question must be 6marks) -- 30 Questions must be covered all possible section. **Section:2** Q-2 (Must be from topics: 1 and 2 (6+6)) Q-3 (Must be from topics: 3 and 4(6+6)) Q-4 (Must be from topic: 5(6))	

Note: Version 1.0.0.0 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme,Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision) L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work

CE= Continuous Evaluation, SEE= Semester End Examination

GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATIONS

Programme	M.Sc.IT(Cyber Security)				Branch/Spec.	DCS		
Semester	I				Version	1.0.0.0		
Effective from Academic Year			2018-19		Effective for the batch Admitted in			June 2018
Subject code	P71A3LF		Subject Name		LINUX FUNDAMENTALS			
Teaching scheme					Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	-	2	-	5	Theory	40	60	100
Hours	3	-	4	-	7	Practical	20	30	50

Pre-requisites:

Overview of operating system, Client-server based Computer Network

Learning Outcome:

By the end of this module students should be able to

- learn about functionalities of secure operating system linux
- understand various package configuration and virtualization
- learn linux administration and management

Theory syllabus

Unit	Content	Hrs
1	**Overview of Linux Operating System** Linux History, Linux features,Linux VS Windows, Linux VS Unix, GNU, Virus free linux, Linux Distribution, Linux Pros and Cons, Root, Linux Commands(cat, touch, ls, du, grep, less, more, pwd), Editors(vi,nano, vim, gedit), Linux Installation, Linux directory structure, Linux Administration, Software Installation	9
2	**Linux initial setup and Booting Process** Mount and Unmount Device, User Administration: Managing Local User and group(create, manage, permissions), Boot Loaders, inittab, rc.sysinit, Service controlling and Demons, Monitoring system: CPU, RAM, HDD, Modules, Logs, Shell Scripting	9
3	**Logical Volume Manager (LVM) and Package Management** Introduction to LVM, YUM package management, RPM package management, Configuring FTP Server, Configuring NFS Server, Configuring Samba Server, Configuring Apache Web-Server, Configuring DHCP Server, DNS Server configuration, Configuring MySQL Database Server	9

4	**Linux Network Management** IPV4, IPV6, IP assigning, MAC, Bridging, Raid protocols, Linux remote connection: (Remote login, transfer file), Remote session(OpenSSh Configuration), Logs introduction, log files(Messages, dmesg, Audit log), cron	9
5	**Security and Network Administration** Virtualization, Understanding attack techniques, Firewall, mod_evasive, iptables, ssh security, tcpwrappers, SELinux, Wireshark and TCPdump, Server and client administration(LDAP, Kerberos, NIS), Process Management	9
Practical content		
List of programs specify by subject teacher based on above mention topics.		
Text Books		
1	Linux Bible Edition 8 By Christopher Negus and Christine Bresnaham Publication Wiley-India	
Reference Books		
1	Fedora Bible 2010 Edition: Featuring Fedora Linux 12	
Note for Examiner		
	Q-1 must be common from any topics from syllabus. Q-2 and onwards must be from specific topics and internal choice or option can be given	
Paper Structure		
	Section :1 Q-1 (Attempt any Five Out of Seven: each question must be 6marks) -- 30 Questions must be covered all possible section. **Section:2** Q-2 (Must be from topics: 1 and 2 (6+6)) Q-3 (Must be from topics: 3 and 4(6+6)) Q-4 (Must be from topic: 5(6))	

Note:

Version 1.0.0.1 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme,Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision)

L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work

CE= Continuous Evaluation, SEE= Semester End Examination

GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATONS

Programme	M.Sc.IT(Cyber Security)		Branch/Spec.	DCS	
Semester	I		Version	1.0.0.0	
Effective from Academic Year	2018-19		Effective for the batch Admitted in	July 2018	
Subject code	P71B4CLI	Subject Name	CYBER LAW AND INDIAN IT ACT		

Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	-	-	-	03	Theory	40	60	100
Hours	3	-	-	-	03	Practical	-	-	-

Pre-requisites:

Required Knowledge of Information Technology

Learning Outcome:

-Able to identify the law against cyber offense
-Investigate cybercrime and collect evidences
-Knowledge about Indian IT act and International law

Theory syllabus

Unit	Content	Hrs
1	**Introduction** Basics of Law, Understanding Cyber Space, Defining Cyber Laws, Scope and Jurisprudence, Concept of Jurisdiction, Cyber Jurisdiction, Overview of Indian Legal System, Introduction to IT Act 2000, Amendments in IT Act, Cyber Laws of EU – USA – Australia - Britain, other specific Cyber laws.	8
2	**Computer Ethics, Privacy and Legislation** Computer ethics, moral and legal issues, descriptive and normative claims, Professional Ethics, code of ethics and professional conduct. Privacy, Computers and privacy issue, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT, Legal Policies, legislative background	8
3	**Intellectual Property Rights Issues** Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property Rights, Understanding Patents, Understanding Trademarks, Trademarks in Internet, Domain name registration, Software Piracy, Legal Issues in Cyber Contracts, Authorship, Document Forgery.	8
4	**Indian IT Act and Standards** Indian IT ACT, Adjudication under Indian IT ACT, IT Service Management Concept, IT Audit standards, ISO/IEC 27000 Series, COBIT, HIPPA, SOX, System audit, Information security audit, ISMS, SoA (Statement of Applicability), BCP (Business Continuity Plan), DR (Disaster Recovery), RA (Risk Analysis/Assessment)	8

5	**International Laws governing Cyber Space** Introduction to International Cyber Law, UNCITRAL, Cyber Laws: Legal Issues and Challenges in India, Net neutrality, Role of INTERPOL.	8
Text Books		
1	Deborah G Johnson, "Computer Ethics"	
2	Cyber Law Simplified by Sood	
Reference Books		
1	Cyber frauds, cybercrimes & law in India by Pavan Duggal	
2	The Internet Law of India: Indian Law Series by Shubham Sinha	
3	Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", Cengage Learning Pub., 2012.	
	Question Paper Scheme: **Note for Examiner** Q-1 must be common from any topics from syllabus. Q-2 and onwards must be from specific topics and internal choice or option can be given **Paper Structure** **Section - 1** Q-1 (Attempt any Five Out of Seven: each question must be 6 marks) --- 30 **Section - 2** Questions must be covered all possible section. Q-2 (Must be From topics: Introduction and Computer Ethics, Privacy and Legislation (12 marks)) Q-3 (Must be From topics: Intellectual Property Rights Issues and Indian IT Act and Standards (12 marks)) Q-4 (Must be From topic: International Laws governing Cyber Space (6 marks))	

Note: Version 1.0.0.0 (First Digit= New syllabus/Revision in Full Syllabus, Second Digit=Revision in Teaching Scheme, Third Digit=Revision in Exam Scheme, Forth Digit= Content Revision)

L=Lecture, TU=Tutorial, P= Practical/Lab., TW= Term work, DT= Direct Teaching, Lab.= Laboratory work

CE= Continuous Evaluation, SEE= Semester End Examination