GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATIONS

Programme	M.Sc.IT(Cyber Security)	Branch/Spec.	DCS
Semester	II	Version	1.0.0.0
Effective from Academic Year	2018-19	Effective for the batch Admitted in	July 2018
Subject code	P72A1PP	Subject Name	Python Programming

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:

Knowledge of basic programming concepts

Learning Outcome:

Understand the fundamental programming concepts of Python
Learn Programming of Network Communication
Use Scapy Python Tool for security testing
Handle error and exception in Python code

Theory syllabus

Unit	Content	Hrs
1	**Introduction to Python :** Installation and working with Python, Features of Python, The Basics: Literal Constants, Numbers, Strings, Variables, Identifier Naming, Data Types, Objects, Logical and Physical Lines, Indentation, Operators and Expressions, Control Flow statements: if, while loop, for loop, break, continue, Library: NumPy, Pandas	9
2	**Using Modules and Data Structures :** Modules: Introduction, The from..import statement, Creating your own Modules, Data Structures: List, Tuple, Dictionary, Sequences, Object-Oriented Programming: classes, objects, The Self, object Methods, The __init__method, Class and Object Variables, Inheritance, polymorphism, Exceptions: Errors, Handling Exceptions, Raising Exceptions, Using Finally	9
3	**String and File Manipulation :** String Functions, Manipulating files and directories, Text files: reading/writing text and numbers from/to a file, creating and reading a formatted file (csv or tab-separated)	9
4	**Network Programming :** Introduction to Sockets, Socket Module, Socket Methods, TCP Socket, Viewing Socket State, Handling Received Client Data over TCP Socket, Blocking and Non-Blocking Socket I/O, Securing Socket, Building a Port Scanner, Application Banner Grabbing, Building an Anonymous FTP Scanner with Python, Using Ftplib to Brute Force FTP	9

	User Credentials	
5	**Scapy – A Python Tool For Security Testing :** Introduction to Scapy, Installation and Platform Specific Instructions, Features of Scapy, Usage of Scapy – Stacking layers, Reading PCAP Files, Generating sets of Packets, Sending Packets, Fuzzing, Send and receive packets (sr() function), TCP traceroute, Packet Sniffing, Importing and Exporting Data	9
Practical content		
List of programs specify by subject teacher based on above mention topics.		
Text Books		
1	Fundamental of Python: First Programs By Kenneth A. Lambert	
Reference Books		
1	A Byte of Python By Swaroop C H	
2	Programming Python By Mark Lutz	
3	Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers By TJ. O'Connor	
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 2.0.0.0 (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	II	Version	1.0.0.0
Effective from Academic Year	2018-19	Effective for the batch Admitted in	July 2018
Subject code	P72A2CF	Subject Name	Cyber Forensic-I

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:

Required Knowledge of various types of cyber-crimes.
Required Knowledge of major operating system.

Learning Outcome:

-Get in depth knowledge of Volume Analysis & File Systems
-Investigate cybercrime and collect evidences
-Able to use proprietors and open source forensic tools

Theory syllabus

Unit	Content	Hrs
1	**Digital Forensic and Investigation** Brief history of digital investigation, Systematic approach of investigation, Digital crime scene evaluation process, Search & Seizure, Digital Forensic Lab Setup, Linux environments for digital forensic investigation (CAINE / Kali etc.), Types of Digital Evidences, Disk Imaging, Write Blockers, Data Recovery, Chain of Custody, Slack Space, Virtual paging, Volatile Evidence Acquisition, Collection & Analysis	9
2	**Volume Analysis & File Systems** Introduction, PC based partitions- DOS partitions, UNIX partitions, RAW partition, UNIX Console Log, Removable media, Server based partitions- BSD partitions, GPT & MBR partitions, multiple disk volumes- RAID, Disk Spanning, file system, File system category, FAT concepts and analysis, FAT data structure- Boot sector, FAT 32 FS info, Directory entries, Long file name directory entries, NTFS File System concepts, NTFS Analysis, NTFS data structure, Standard file attributes, Index attributes and data structures	9

3	**Forensic Tools** Kali Linux (Binwalk, bulk-extractor, Capstone, chntpw, Cuckoo, dc3dd, ddrescue, DFF, diStorm3, Dumpzilla, extundelete, Foremost, Galleta, Guymager, iPhone Backup Analyzer, p0f, pdf-parser, pdfid, pdgmail, peepdf, RegRipper, Volatility, Xplico), Introduce with CAINE forensic environment and major forensic tools, Open source forensic tools, Developing scripted tools for basic level investigation, Windows Forensic Analysis **-** File analysis, Registry Analysis	9
4	**Digital Evidence Analysis** Potential Evidences, Evidence collection form different devices, Artifact interpretation, Operating System artifacts analysis, Network Artifacts analysis, File Signatures, Registry Forensics, Last user Activity, MRU, NTUSER.DAT, MFT concepts, MFT Forensics, Multimedia Forensics, Metadata Analysis, Browser Forensics, History Extraction, Cookies based artifacts, Autofill Forms, Cache, Temp file, MAC OS Artifacts analysis, Linux OS Artifact Analysis, Volatile Memory based Artifacts	9
5	***NIX File Systems** UNIX, Ext2 and Ext3 data structures, iNodes, Super block, group descriptor tables, Block bitmap, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures, UFS1 and UFS2 concepts and analysis, NFS Files Systems, HFS File Systems, CDF File systems, Hadoop File systems	9
Practical content		
List of programs specified by the subject teacher based on above mentioned topics		
Reference Books		
1	Guide to Computer Forensics and Investigations, Fourth Edition by Bill Nelson, Amelia Phillips, Christopher Steuart	
2	Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8 by Harlan Carvey	
3	Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey	
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.	
Semester	II	Version	1.0.0.0
Effective from Academic Year	2018-19	Effective for the batch Admitted in	July 2018
Subject code	P72A3WP	Subject Name	Web Pentesting

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:

Basic knowledge of Metasploit framework.
Client and Server Scripting technology.
Coding of Java Script, PHP script
Any computer programing language

Learning Outcomes:

To understand different types of web application attacks.
To understand use metasploit framework for securing web.
To understand to apply several testing to check security on web application.

Theory syllabus

Unit	Content	Hrs
1	**Input Validation Testing** Testing for Reflected Cross Site Scripting, Testing for Stored Cross Site Scripting, Testing for HTTP Verb Tampering, Testing for HTTP Parameter pollution, Testing for SQL Injection, Testing for LDAP Injection, Testing for XML Injection, Testing for Code Injection,	9
2	**vulnerability scanner:** The Basic Vulnerability Scan, Scanning with NeXpose, Scanning with Nessus, Specialty Vulnerability Scanners, Using Scan Results for Auto ping **Exploitation:** Basic Exploitation, Exploiting Your First Machine, Exploiting an Ubuntu Machine, All-Ports Payloads: Brute Forcing Ports, Resource Files, Wrapping Up.	9

3	**Meterpreter:** Compromising a Windows XP Virtual Machine, Dumping Usernames and Passwords, Pass the Hash, Privilege Escalation, Token Impersonation, Using ps, Pivoting onto Other Systems, Using Meterpreter Scripts, Leveraging Post Exploitation Modules, Upgrading Your Command Shell to Meterpreter, Manipulating Windows APIs with the Railgun, Wrapping Up,	9
4	**Session Management Testing** Testing for Bypassing Session Management Schema, Testing for Cookies attributes, Testing for Session Fixation, Testing for Exposed Session Variables, Testing for Cross Site Request Forgery (CSRF), Testing for logout functionality, Test Session Timeout.	9
5	**Client Side Testing** Testing for Client Side URL Redirect, Testing for Clickjacking, Test Cross Origin Resource Sharing, Testing for Spoofable Client IP address	9
Practical content		
List of programs specify by subject teacher based on above mention topics.		
Text Books		
1	-Metasploit The Penetration Tester's Guide - David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni	
Reference Books		
1	The Web Application Hecker's Handbook 2 – Dafydd Stuttard , Marcus Pinto	
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))	

GANPAT UNIVERSITY									
FACULTY OF COMPUTER APPLICATIONS									
Programme	M.Sc.IT(Cyber Security)					Branch/Spec.	DCS		
Semester	II					Version	1.0.0.0		
Effective from Academic Year				2018-19		Effective for the batch Admitted in			July 2018
Subject code	P72B4CN			Subject Name		Computer Network Operation			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture(DT)		Practical(Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	3	-	-	-	3	Theory	40	60	100
Hours	3	-	-	-	3	Practical	-	-	-

Pre-requisites:

Basic Information of Computer Networking and Communication, Unguided and Guided Media of Computer Network

Learning Outcome:

By the end of this module students should be able to

- Learn about computer network and its usability
- Understand various Network Communication Protocols.
- Acquired the knowledge of network security

Theory syllabus

Unit	Content	Hrs
1	**Fundamental of Computer Network** Network Types, Work group model VS Domain Model, Network Topologies, Types of Server, Computer Network connecting Devices, VLAN configuration in switch, wired and wireless Networks, OSI Model, TCP / IP Reference models, IEEE standards, Firewall authentication	9
2	**Networking Host Layers:** Application Layer: SIP, NNTP, FTP, HTTP, NFS, NTP, SMPP, SMTP, SNMP, Telnet, Presentation Layer: MIME, SSL, TLS, XDR, Session Layer: Sockets, Session establishment in TCP, RTP, PPTP, Transport Layer: SCTP, DCCP, UDP, TCP, TCP Connection Establishment and Termination.	9

3	**Networking Media Layers:** Network Layer: IPv4, IPv6, IP Address Classes, Subnet Masks and CIDR Networks, IPsec, ICMP, IGMP, OSPF(Link State), Distance Vector(RIP), Data Link Layer: PPP, SBTV, SLIP, Physical Layer: X.25, wifi, Ethernet, FDDI	9
4	**Computer Network Administration:** Introduction to server Operating System, DNS, DNS forward lookup zone and reverse lookup zone, Managing User and Group, Introduction to DHCP, DHCP configuration, Group Policy	9
5	**Server Virtualization and Security Authentication** Introduction to virtualization, virtualization Architecture, System Backup and recovery, Security Protocols, Security threads, overview of system troubleshooting	9
Text Books		
	TCP/IP Protocol suite B.A. Forouzan Microsoft server 2008: beginner's guide Marty Matthews published by McGraw hill	
Reference Books		
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