GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATIONS

Programme	M.Sc. IT(Cyber Security)	**Branch/Spec.**	Computer Applications
Semester	III	**Version**	1.0.0.0
Effective from Academic Year	2019-20	**Effective for the batch Admitted in**	June 2018
Subject Code	P73A1MTA	**Subject Name**	Malware Taxonomy and Analysis

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

Objective:

To learn the use of various tools and tricks to perform basic static analysis to identify, detect and eliminate malware attacks. To learn live malware attack monitoring and analysis as well live network traffic analysis.

Pre-requisites:

Required Knowledge of C and C++. Required Knowledge of Assembly Language.

Learning Outcome:

After completing this course, students should be:

- ✓ Aware about malware and its analysis methodology
- ✓ Able to perform basic static analysis with various tools
- ✓ Able to perform analysis in protected environment
- ✓ Able to perform basic dynamic analysis
- ✓ Monitoring Network with Wireshark
- ✓ Aware with various types of malware and its functionalities

Content:

Unit		Hrs
1	**Malware Analysis Introduction** What is Malware?, Types of Malware, The goal of Malware analysis, Malware Analysis Methodology, What is Malware Analysis?, Basic Techniques for Malware Analysis, General Rules for Malware Analysis, Lab Setup for Malware Analysis	9
2	**Basic Analysis** Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executables File Format, Linked Library and Functions, Static Analysis in Practice, The	9

	PE File Headers and Section	
3	**Malware Analysis in Virtual Machine** The Structure of Virtual Machine, Creating Malware Analysis Machine, Using Malware Analysis Machine, Risk of Virtual Machine for Malware Analysis.	9
4	**Basic Dynamic Analysis** Malware Sandboxes, Monitoring with Process Manager, Viewing Process with Process Explorer, Comparing Registry Snapshot, Faking a Network, Packet Sniffing with Wireshark, Using INetSim.	9
5	**Malware Functionality** Malware Behaviour: Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanism, Privilege Escalation.	9
Practical Content:		
List of programs specified by the subject teacher based on above mentioned topics		
Reference Books:		
1	Practical Malware Analysis by Michael Sikorski and Andrew Honig, No Starch Press, 2015	
Web Reference:		
Question Paper Scheme:		
	University Examination Duration: 3 Hours 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. **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.**	Computer Applications
Semester	III	**Version**	1.0.0.0
Effective from Academic Year	2019-20	**Effective for the batch Admitted in**	June 2018
Subject Code	P73A2MDS	**Subject Name**	Mobile Device Security and Forensic

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

Objective:

To help students learn, understand, and practice mobile security, which include the study of android pentest and reversing android application. Discover leakages and vulnerabilities in mobile device application.

Pre-requisites:

Required Knowledge of Mobile Device, Required Knowledge of Java and Android Technology.

Learning Outcome:

After completing this course, students should be able to:

- ✓ Create basic Android app. architecture.
- ✓ Understand the Android security.
- ✓ Do the Pentesting in Android app.
- ✓ Analyze Android traffic interception.
- ✓ Do the data extraction on Android based smartphone.

Content:

Unit		Hrs
1	**Introduction Android** Basics of Android, Android SDK Installation, The Android O/S Architecture, AVD, Activity and Its Lifecycle, Create an Activity, Intent: Implicit Intent, Explicit Intent, Android Manifest, User Input Controls	9
2	**Android Security** Digging deeper into Android, Sandboxing and the permission model, Application signing, Android startup process, Useful utilities for Android Pentest, Android Debug Bridge, Burp Suite, APKTool	9
3	**Reversing and Auditing Android Apps** Android application teardown, Reversing an Android application, Using APKTool to	9

	reverse an Android application, Auditing Android applications, Content provider leakage, Insecure file storage, Path traversal vulnerability or local file inclusion, Client-side injection attacks	
4	**Traffic Analysis** Android traffic interception, Ways to analyse Android traffic: Passive analysis, Active analysis, HTTPS Proxy interception: Other ways to intercept SSL traffic, Extracting sensitive files with packet capture	9
5	**Android Forensics** Types of forensics, Filesystems: Android filesystem partitions, Using dd to extract data: Using a custom recovery image, Using Andriller to extract an application's data, Using AFLogical to extract contacts, calls, and text messages, Dumping application databases manually, Logging the logcat, Using backup to extract an application's data	9

Practical Content:
List of programs specified by the subject teacher based on above mentioned topics

Reference Books:	
1	Android Developer Fundamental: Concept Reference By Google Developer
2	Team Learning Pentesting for Android Devices by Aditya Gupta, Published by Packt Publishing Ltd.
3	Android Wireless Application Development By Shane Conder & Lauren Darcy, Addison-Wesley Publication

Web Reference:	
1	https://developer.android.com/studio

Question Paper Scheme:	
	University Examination Duration: 3 Hours 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. **SECTION – I** Q-1 (Attempt any Five Out of Seven: each question must be 6 marks) – 30 Questions must be covered all possible section. **SECTION – II** 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.(CA&IT)	**Branch/Spec.**	Computer Applications
Semester	III	**Version**	1.0.0.0
Effective from Academic Year	2019-20	**Effective for the batch Admitted in**	June 2018
Subject Code	P73A3NF	**Subject Name**	Network Forensic

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

Objective:

To learn the fundamentals of Network Security and Network Forensic. This course provides a practical hands-on introduction to developing network forensic framework. The tools to record and analyze network logs have been explored.

Pre-requisites:

Required Knowledge of Computer Network Fundamental.
Required Knowledge basic knowledge of Communication devices.

Learning Outcome:

After completing this course, students should be able to:

- ✓ Fundamentals of Network Security and Forensic
- ✓ Network Forensic Model,
- ✓ Tools related with Network Forensics, Vulnerability assessment
- ✓ Network monitoring , Scanning and Network Forensics

Content:

Unit		Hrs
1	**Network Forensics** Introduction, Classification of Network Forensic Systems, Recent Trends in Network Forensics: Steganography, Honeypot Forensics, IP Version 6 Forensics, Botnet Forensics, Wireless Network Forensics, Application Layer Forensics, Challenges in Network Forensic Analysis	9
2	**Network Forensic Process Models** Digital Forensic Process Models, Hierarchical Process Model, Network Forensic Process Models, Generic Process Model for Network Forensics **Network Forensic Frameworks** Distributed Systems-Based Frameworks, Soft Computing-Based Frameworks, Honeynet-Based Frameworks, Attack Graph-Based	9

	Frameworks, Formal Method-Based Frameworks, Aggregation-Based Frameworks, Data Mining-Based Frameworks	
3	**NFAT** NetDetector, NetIntercept, OmniPeek, PyFLAG, Xplico **VAT** Metasploit, Nessus, Yersinia	9
4	**Network Sniffing and Packet Analyzing Tools** Wireshark, Aircrack-ng, WebScarab, NetworkMiner, Kismet **Network Scanning Tools** Nmap, Angry IP Scanner, **IDS** Snort	9
5	**Network Forensic Acquisition** TCP/IP Protocol Suite, Packet Capture Format, pcapng Dump File Format, NetFlow Record Format	9
Practical Content:		
List of programs specified by the subject teacher based on above mentioned topics		
Reference Books:		
1	Fundamentals of Network Forensics A Research Perspective, By R.C. Joshi & Emmanuel S. Pilli Published By Springer ISSN 1617-7975	
2	Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools 1st Edition, Packt Publishing by Nipun Jaswal	
3	Digital Forensics for Network, Internet, and Cloud Computing by Clint P. Garrison, Craig A. Schiller, James Steele by Syngress	
Question Paper Scheme:		
	University Examination Duration: 3 Hours 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. **SECTION – I** Q-1 (Attempt any Five Out of Seven: each question must be 6 marks) – 30 Questions must be covered all possible section. **SECTION – II** 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.**	Computer Applications
Semester	III	**Version**	1.0.0.0
Effective from Academic Year	2019-20	**Effective for the batch Admitted in**	June 2018
Subject Code	P73A4IP1	**Subject Name**	INDUSTRIAL PROJECT – I

Teaching scheme						**Examination scheme (Marks)**			
(Per week)	**Lecture (DT)**		**Practical (Lab.)**		**Total**		**CE**	**SEE**	**Total**
	L	TU	P	TW					
Credit	-	-	5	-	5	Theory	-	-	-
Hours	-	-	5	-	5	Practical	150	100	250

Objective:

Industrial Project -I course is an organized method or activity of enhancing and improving skill set and knowledge of computer science students which boost their performance and consequently helping them to meet their career objectives. Industrial Project is crucial for students because it is the best way to acquire as much mastery about their field as possible which helps in building confidence of the students.

Pre-requisites:

SDLC, Models for Software Engineering, OOPs, Basic DBMS concepts, Design Techniques like DFD or UML etc., Basic Information of Business Processes according to project title.

Learning Outcome:

- Understanding of how system is analyzed and implemented using standard techniques.
- Design and Implementation of proposed system
- Testing the system
- Deployment of the system

Content:

Unit		Hrs
	Rules: • The project development shall be carried out along with the regular subject in curriculum during the semester. The students can develop their project individually or in a group of not more than 2 students. Group size can be increased with prior approval of head of institution. • The passing standard is 40% in internal and external examination jointly. • The detail study of any enterprise application or any major IT infrastructure setup can also be accepted as a project work. The project can be developed in any language or platform but it is required to get approved by the head of the institution. For the purpose of approval, Students have to submit their project	

	titles and proposals with the name of internal and external guides to the Head of Institution In case, if the student proposal is rejected, the revised proposal in the same or other area is required to submit and get it sanctioned. Failing to do this, his/her term will not be granted. • The students have to report to the internal guide for at least 4 times during the project life span. Students are required to submit their presentation in soft copy as per format to assigned internal guide at least before 4 days of internal presentation schedule. • The external examiners appointed by the University will give the external marks on the basis of the heads like Presentation, Demonstration, Viva Voce, and Documentation etc. The distribution of marks to different heads may be decided at the time of evaluation of the project but it is expected to have the same distribution. • The Internal Guide or Head of the Institution will give the internal marks. These marks may be given on the bases of regular reporting of the student to the internal guide.	

Examination Weight age:

Internal Examination		**External Examination**	
Internal Head	Weight age (60%)	External Head	Weight age (40%)
Presentations	25 %	Final Viva Presentation (Project Analysis, Project Designing, Technical aspects etc.)	25 %
Project Analysis	10 %		
Project Designing	10 %		
Technical aspects	10 %		
Project Outcomes	5 %	Report Submission	15%

GANPAT UNIVERSITY

FACULTY OF COMPUTER APPLICATIONS

Programme	M.Sc. IT(Cyber Security)	**Branch/Spec.**	Computer Applications
Semester	III	**Version**	1.0.0.0
Effective from Academic Year	2019-20	**Effective for the batch Admitted in**	June 2018
Subject Code	P73B5ISC	**Subject Name**	Information Security Compliance Management

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	-	-	-

Objective:

- To learn about Information Security, its Management and Implementation.
- To aware the students about the various standards for Information Security.
- To awake the learners regarding IPR and Professional Ethics and their importance.

Pre-requisites:

Required Knowledge of Information Security.

Learning Outcome:

The Students should be able to learn concepts of,

- ✓ Information Security Management System and its implementation
- ✓ Information Security Standards
- ✓ IPR and Professional Ethics

Content:

Unit		Hrs
1	**Information Security and Management** What is Information Security? Need for Information Security, Information Security Management System (ISMS), Benefits of Information Security Management System, Principles of Information System Security, Information classification, Security Policies, Various standards, models and frameworks for Information Security.	8
2	**ISO/IEC 27001 Standards** ISO/IEC 27001 specification, Stages of ISO 27001 process (PDCA approach), ISMS Risk management, Key contexts of ISO 27001, ISO 27001 certification process, Benefits of ISO 27001 certification, Overview of different clauses of ISO/IEC 27001.	9
3	**ISMS Implementation** Organization of Information Security, Asset Management, Different Communication and Operation Management, Access Control, Establish, Monitor, Maintain and Improve	10

	ISMS, Planning and conducting ISO/IEC 27001 audit, Internal ISMS Audit, Organizational Responsibilities for ISMS.	
4	**Information Security Compliance Standards** Overview of different Information Security Compliance Standards, HIPAA (Health Insurance Portability and Accountability Act) – Purpose, Privacy and Security Rule, PCI – DSS (Payment Card Industry Data Security Standard) – Goals, PIN Transaction Security (PTS), Payment Application Data Security Standard (PA-DSS).	9
5	**IPR (Intellectual Property Rights) & Professional Ethics** Introduction of IPR. Advantages of IPR, Different types of IPR, IPR in India, IPR in Abroad. **Professional Ethics** Ethics in Information Security, Need for Ethics in Information Security, Code of Ethics for Information Security Experts.	9

Practical Content:

Reference Books:	
1	Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Nina Godbole, Wiley.
2	ISO27001 / ISO27002 A Pocket Guide, Alan Calder, IT Governance Publishing.
3	Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000, International Standards.
4	Information Security Management Standards: Compliance, Governance and Risk Management, Edward Humphreys, 2008 Published by Elsevier Ltd.

Web Reference:	

Question Paper Scheme:	
	University Examination Duration: 3 Hours 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. **SECTION – I** Q-1 (Attempt any Five Out of Seven: each question must be 6 marks) – 30 Questions must be covered all possible section. **SECTION – II** 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))