3rd Semester

 # Only in case offline classes are not possible due to reasons like COVID Pandemic the classes will be in synchronous online mode

Subject Type	Course Name	Course Code	Credit Distribution			Credit Points	Mode of Delivery			Proposed Moocs
			Theory	Practical	Tutorial		Offline#	Online	Blended	
CC 5	Ethical Hacking and Systems Defence	CYS (T) 301	4	0	0	6	✓			As per MAKAUT Notification
		CYS 391	0	2	0					
CC 6	Cyber Systems & Cyber Threat and Modelling	CYS (T) 302	4	0	0	6	✓			
		CYS 392	0	2	0					
CC 7	Vulnerability Analysis, Penetration Testing, and Incident Handling	CYS (T) 303	4	0	0	6	✓			
		CYS 393	0	2	0					
GE 3	Students will have to choose from the GE Basket					6			✓	
SEC 1	Operating System and Linux	CYS 354	0	2	0	2	✓			
Semester Credits						**26**				

CYS 301- Ethical Hacking and Systems Defence

Credits- 4L+2P

Course Objective: The course is designed to provide an elaborate idea about the different system hacking techniques with proper ethics and applying system defence techniques.

Sl	Course Outcome	Mapped modules
1	Understand and experiment with ethical hacking.	M1
2	Understand and experiment with system hacking.	M2
3	Make use of TCP/IP overview concepts and port scanning.	M3
4	Analyse desktop and server operating systems(OS) vulnerabilities.	M4
5	Assess details of system and network security.	M5
6	Inspect vulnerabilities in OS.	M6

Theory – CYS(T) 301

Mapped Modules	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Introduction to Ethical Hacking	10	25	1,2,3	
M2	System Hacking	14	25	1,2,3	
M3	TCP/IP Overview Concepts and Port Scanning	14	30	2,3	
M4	Desktop and Server OS Vulnerabilities	10	20	3,4	
		48	**100**		

Practical- CYS 391

Mapped Modules	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	System and Network Security	14	60	3,4,5	
M6	Identifying vulnerabilities in OS	14	40	3,4,5	
		28	**100**		

Ethical Hacking and Systems Defence

MODULE 1: INTRODUCTION TO ETHICAL HACKING:
Introduction: Hacking/ Ethical hacking, Types of Hacking/Hackers, Cybercrime, Types of cybercrime, Hacker Mind set, Threats, Concept of ethical hacking, Phases involved in ethical hacking, Role of Ethical Hacking, Common Hacking Methodologies, Profiles of Hackers, Benefits of Ethical Hacking, Limitations of Ethical Hacking, Foot printing-Social Engineering-Scanning and enumeration

MODULE 2: SYSTEM HACKING:
System hacking, Types of System hacking, ha4cking tools, Computer Hole, Hacking Process, Various methods of password cracking, Remote Password Guessing, Role of eavesdropping, Keystroke Loggers, Types of Keystroke Loggers, Detection, Prevention and Removal, Rootkits-Trojans-Backdoors-Viruses and worms, sniffers-denial of service-Session hijacking.

MODULE 3: TCP/IP OVERVIEW CONCEPTS AND PORT SCANNING:
Review of TCP/IP Internetworking, Networking and Security Overview, Attack Methods, Access Control and Site Security, Host Security, Security issues in Internet protocols: TCP, DNS, and routing, Overview of TCP/IP-IP addressing-numbering systems- Introduction to port scanning-types of port scan port scanning tools-ping sweeps- Understanding scripting-Enumeration.

MODULE 4: DESKTOP AND SERVER OS VULNERABILITIES: OS Security Vulnerabilities, Programming Bugs and Malicious code, Windows OS vulnerabilities-tools for identifying vulnerabilities in windows-Linux OS vulnerabilities, vulnerabilities of embedded OS.

MODULE 5: System and Network Security: Desktop Security, Operating System Security: Designing Secure Operating Systems, Understanding routers-understanding firewalls-risk analysis tools for firewalls- understanding intrusion and detection and prevention systems-honeypots, Disaster recovery, Digital Signature, International Standards maintained for Cyber Security, Security Audit, and Investigation by Investing Agency.

Module 6: Practical: Identifying vulnerabilities in OS, Computer Forensics, Practical: hacking the server (through virtual machine), Micro Project.

Suggested Readings

1 Michael T. Simpson, Kent Backman, James Corley ―Hands-On Ethical Hacking and Network Defense‖,2016
2 Steven DeFino, Barry Kaufman, Nick Valenteen ―Official Certified Ethical Hacker Review Guide‖,2015
REFERENCE BOOKS 1 The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series)
E BOOKS: https://www.nationalcyberwatch.org/resource/ethical-hacking-systems-defense-nationalcyberwatch-center-edition/

CYS 302- Cyber Systems & Cyber Threat and Modelling

Credits- 4L+ 2P

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome	Mapped Module/s(if applicable)
1.	Understand threat models by discussing strategies and structured approaches to threat modelling.	M1
2.	Apply different processes(such as finding, spoofing, tampering etc.) to the threats.	M2
3.	Make use of different techniques for managing and addressing the threats.	M3
4.	Explain and Identify different threat modelling tools.	M4
5.	Evaluate different threats to cryptosystems.	M5
6.	Appraise different intrusion and detection techniques.	M6

Theory- CYS(T) 302

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Dive In and Threat Model	12	25	1,2	
M2	Finding Threats	12	30	2,3	
M3	Managing and Addressing Threats	12	30	2,3	
M4	Threat Modelling Tools	12	15	2,3	
		48	**100**		

Practical- CYS 392

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Threats to Cryptosystems	14	60	3,4,5	
M6	Intrusion and detection techniques	14	40	3,4,5	
		28	**100**		

Cyber Systems & Cyber Threat and Modelling

Module-1: Dive in and Threat Model, learning to Threat Model. Strategies for Threat Modelling, Brainstorming Your Threats, Structured Approaches to Threat Modelling, Models of Software,

Module-2: Finding Threats, STRIDE, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats. Attack Trees, Working with Attack Trees, Representing a Tree, Real Attack Trees. Attack Libraries, Properties of Attack Libraries.

Module-3 Managing and Addressing Threats, Processing and Managing Threats, Starting the Threat Modelling Project, Digging Deeper into Mitigations, Tracking with Tables and Lists, Scenario-Specific Elements of Threat Modelling. Defensive Tactics and Technologies, Tactics and Technologies for Mitigating Threats, Addressing Threats with Patterns, Mitigating Privacy Threats.

Module-4 Threat Modelling Tools, Generally Useful Tools, Open-Source Tools, Commercial Tools. Web and Cloud Threats, Web Threats, Cloud Tenant Threats, Cloud Provider Threats, Mobile Threats.

Module-5 Threats to Cryptosystems, Cryptographic Primitives, Classic Threat Actors, Attacks against Cryptosystems, building with Crypto, Things to Remember about Crypto Experimental Approaches, looking in the Seams, Operational Threat Models, Threats to Threat Modelling Approaches, How to Experiment.

Module 6: Intrusion and detection techniques, Programming Bugs and Malicious code, E-commerce Security, web browser security, Mini Project.

Suggested Readings:

1. Adam Shostack, “Threat Modelling: Designing for Security Designing for Security” Wiley publication, Edition, 2008.
2. Frank Swiderski, Window Snyder “Threat Modelling (Microsoft Professional)” Microsoft Press, Edition, 2008.

CYS 303- Vulnerability Analysis, Penetration Testing, and Incident Handling

Credits- 4L+2P

Course Objective: The course is designed to provide competencies about the different cyber systems issues and different threat modelling systems.

Sl. No.	Course Outcome	Mapped Module/s(if applicable)
1.	Demonstrate details of vulnerability.	M1
2.	Make use of and penetration testing overview.	M2
3.	Examine the details of cyber security incident management.	M3
4.	Test for ethical hacking.	M4
5.	Test for and evaluate vulnerability assessment tool.	M5
6.	Determine and design different hacking techniques.	M6

Theory- CYS (T) 303

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Vulnerability	12	25	1,2	
M2	Introduction to Penetration Testing, Penetration Testing Overview	12	25	2,3	
M3	Cyber Security Incident Management	12	25	2,3,4	
M4	Ethical Hacking	12	25	2,3,4	
		48	**100**		

Practical- CYS 393

Module No	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M5	Working of Vulnerability Assessment Tool	14	50	3,4,5	
M6	Hacking Techniques	14	50	3,4,5,6	
		28	**100**		

Vulnerability Analysis, Penetration Testing, and Incident Handling

Module 1: Vulnerability - Introduction, Overview of Security threats and Vulnerability, Benefits, Methodology, Vulnerability and Threats, Malware: Viruses, Worms, Trojan horses, Security Vulnerabilities Types of attacks on Confidentiality, Integrity and Availability, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application vulnerability, Security Counter Measures, Intrusion Detection, Antivirus Software Intrusion Detection, Antivirus Software, vulnerability to security risks, Failure to Restrict URL, Remote Code Execution, tools use for vulnerability checking.

Module 2: Introduction to Penetration Testing, Penetration Testing Overview: What is Penetration Testing? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance, Discovery, Analysing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, and Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing. White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing, Conclusion.

Module 3: Cyber security Incident Management: The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist, Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post-Incident Activity, Handling an Incident: Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization & Incident Notification, Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.

Module 4: Ethical Hacking, Penetration Testing, Vulnerability Assessment and Penetration Testing, SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Security Counter Measures, Overview of digital forensics,

Module 5: Working of Vulnerability Assessment Tool, Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration, – vulnerability analysis, Planning and Discovery Knowledge Check, Attack and Reporting.

Module 6: Hacking Techniques, Penetration Testing Tools, Tools use in Incident Response, Incident Response Knowledge.

Suggested Readings:

1. Mastering Modern Web Penetration Testing by Prakhar Prasad, October 2016 Packt Publishing.
2. Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran, Cameron Buchanan,2015 Packt Publishing.

CYS 354- Operating System and Linux
Credits- 2P

Course Objective: The course is designed in order to provide an elaborate idea about different functional components of the Linux Operating System and their various utilities. At the end of the course, the students are expected to know about various functional components of an operating system, their utilities, significance and applications through Linux OS, in order to solve real life problems.

Sl	Course Outcome	Mapped modules
1	Understand the structure, function and applications of basic Linux utilities	M1, M2
2	Understand and apply various file handling utilities and filters in Linux OS	M2, M3
3	Explain the basic structure and implications of advanced file attributes in Linux OS	M3, M4
4	Model the basic structure and utility of the shell interface in Linux OS	M4, M5
5	Develop programming skills in order to work with Linux Shell & Shell Scripting	M4, M5
6	Examine and explain the various OS related functions being implemented by the Linux OS	M5, M6

Module Number	Headline	Total Hours	%age of questions	Blooms Level	Remarks (If any)
M1	Basic LINUX Utilities	4	10%	1,2	
M2	Directory and Ordinary File Handling	4	10%	1,2	
M3	Basic Filters	4	20%	2,3	
M4	File attributes	4	20%	2,3	
M4	Shell and Shell Scripting	6	30%	4,5,6	
M5	Process and Memory management in Linux	4	10%	4,5	
		26	**100**		

Module 1: Basic LINUX Utilities (4 hrs)
Calendar (*cal*), Display system date (*date*), Message display (*echo*), Calculator (*bc*), Password changing (*passwd*), knowing who are logged in (*who*, *w*), Knowing System information (*uname*).

Module 2: Directory and Ordinary File Handling (4 hrs)
Displaying pathname of the current directory (*pwd*), Changing the current directory (*cd*), Make directory (*mkdir*), Remove directories (*rmdir*), Listing contents of directory (*ls* and its options), Absolute pathname, Relative pathname, Referring directories with dot (.) and dot dot (..) identifiers Displaying and creating files (*cat*), Copying a file (*cp*), Deleting a file (*rm*), Renaming/ moving a file (*mv*), Paging output (*less, more*), Knowing file type (*file*), Line, Word & Character counting (*wc*), Comparing files (*cmp*), Finding common between two files (*comm*), Displaying file differences (*diff*)

Module 3: Basic Filters (4 hrs)
Prepare file for printing (*pr*), Horizontal division of file (*head* and *tail)*, Vertical division of file (*cut*), Paste files (*paste*), Sort file (*sort*), Finding repetition and non- repetition (*unique*), Manipulating characters (*tr*), Searching patterns in files (*grep*).

Module 4: File attributes (4 hrs)
File and directory attributes listing, File ownership, File permissions, changing file permissions – relative permission & absolute permission, changing file ownership, changing group ownership, File system and Inodes, Hard link, Soft link, setting Default permissions of file and directory using *umask*, listing of modification and access time, Time stamp changing, File locating.

Module 5: Shell and Shell Scripting (6 hrs)
Types of shell, Pattern matching, Escaping, Quoting, Redirection, Pipe, Tee, Command substitution, Shell variables. Introduction to shell scripting: Simple shell scripts, Interactive shell scripts, using command line arguments, Logical operators (&&, ||), Condition checking (*if-then-fi, if-then-else-fi, if-then—elif-else-fi, case*), Expression evaluation (*test, []),* Computation (*expr*), Using *expr* for strings, Looping (*while*, *for*, *until*, *break*, *continue*), Use of positional parameters. Simple implementation of basic LINUX commands, utilities, filters etc. using shell scripts.

Module 6: Process and Memory management in Linux (4 hrs)
Display process attributes (*top*), Display System processes (*ps*), Changing process priority (*nice*), Listing jobs (*jobs*), Sending jobs to background (bg) and foreground (fg), Killing or terminating processes (*kill*), Inter Process Communication management (*ipcs*), Memory management commands and utilities – *free, df, top, htop, vmstat, dmidecode,* etc.