NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS407CC25
Course Title:	System Administration
Course Type:	Core
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
2	0	4	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to:

1. explain the fundamentals of system booting, process management, and access control in Linux (BL2)
2. demonstrate proficiency in software installation, package management, and user administration using shell scripting (BL2)
3. analyse system logs, monitoring data, and security threats to troubleshoot performance and security issues (BL4)
4. configure security mechanisms, firewalls, and network monitoring tools to enhance system resilience. (BL5)

Unit	Contents	Teaching Hours (Total 30)
Unit-I	**Booting and System Management Daemons:** Overview, System firmware, GRUB, System management daemons, *systemd*, Reboot and shutdown procedures	03
Unit-II	**Access Control and Root Privileges:** UNIX access control, Root account management, Extensions to the standard access control model, Modern access control	03
Unit-III	**Process Control and The File System:** Components of a process, The lifecycle of a process, Process control commands, Periodic processes; File system mounting and unmounting, File types, File attributes, Access control lists	04
Unit-IV	**Software Installation and Management:** Operating System installation, Managing packages, Linux package management systems, High-level Linux package management systems	03
Unit-V	**Scripting, User Management, and Logging:** Shell basics, Shell scripting, Regular expressions, Revision control with Git; Account mechanics, The */etc/passwd, /etc/shadow,* and */etc/group* files, Scripts for user addition and safe removal; Log locations, The *systemd* journal, Syslog, Kernel and boot-time logging, Management and rotation of log files	06
Unit-VI	**Drivers and the Kernel:** Version numbering, Devices and their drivers, Linux Kernel configuration, Loadable Kernel modules, Booting, Booting alternate Kernels in the cloud, Kernel errors	04

Unit-VII	**System Security:** Elements of Security, Reasons for compromised security, Basic security measures, Passwords and user accounts, Security tools, SSH, Firewalls, VPNs, Security standards	04
Unit-VIII	**Monitoring:** Overview, Monitoring platforms, Data collection, Network, Systems, Applications, and Security monitoring, Simple Network Management Protocol.	03

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Evi Nemeth, Garth Snyder, Trent Hein, Ben Whaley, Dan Mackin, UNIX and Linux System Administration Handbook, Addison-Wesley
2. Thomas A. Limoncelli, Christina J. Hogan, Strata R. Chalup, The Practice of System and Network Administration, Addison-Wesley
3. William Shotts, The Linux Command Line, No Starch Press.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	System boot and GRUB configuration i) Explore BIOS/UEFI and system firmware ii) Modify and configure GRUB bootloader settings iii) Boot into single-user mode and troubleshoot boot issues	6
2	User and Access Control Management i) Create and manage user accounts, groups, and permissions ii) Configure sudo access for privilege escalation iii) Implement Access Control Lists (ACLs) and SELinux/AppArmor policies	6
3	Process Control and System Monitoring i) Use commands like ps, top, htop, nice, and kill ii) Schedule periodic tasks using cron and systemd timers iii) Monitor system performance using tools like vmstat, iostat, and mpstat	6
4	File System Management and Mounting i) Create, format, and mount different file systems (ext4, XFS, Btrfs) ii) Implement logical volume management (LVM) iii) Set up disk quotas and analyze file system usage	6
5	Linux Package Management i) Install, update, and remove packages using apt, yum, and dnf ii) Compile and install software from source iii) Manage system dependencies and repositories	6
6	Shell Scripting and Automation i) Write basic and advanced shell scripts using conditional statements, loops, and functions in scripts ii) Automate user management and system tasks	6

7	Logging and System Auditing i) Configure and analyze logs using syslog, journalctl, and rsyslog ii) Implement log rotation with logrotate iii) Audit system security using auditd	6
8	Kernel Management and Driver Modules i) Check and update the Linux kernel ii) Load and unload kernel modules using modprobe iii) Compile and install a custom kernel	6
9	System Security and Network Hardening i) Configure and manage firewalld and iptables ii) Implement SSH hardening and key-based authentication iii) Secure network services using TCP wrappers and intrusion detection tools	6
10	Network and Application Monitoring i) Use SNMP, netstat, iftop, and nmap for network monitoring ii) Analyze system health with Nagios/Zabbix/Prometheus iii) Monitor application logs and detect security breaches.	6