GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering
Level: Diploma
Branch: Cyber System and Information Security
Subject Code: DI03066011
Subject Name: Linux for Security

W.E. F. Academic Year:	2026-27
Semester:	3rd
Category of the Course:	PCC

Prerequisite:	Basic computer literacy, Logical Thinking, Command Line Interface
Rationale:	This course builds directly upon the Linux fundamentals covered in the Fundamentals of Operating System subject and focuses on security-oriented practical skills in Linux. Students will gain hands-on experience in Linux file system administration, user and permission management, process handling, network monitoring, shell scripting, log analysis, and Linux system hardening. With a strong emphasis on cybersecurity tools such as Nmap, Wireshark, tcpdump, UFW, Fail2Ban, Hydra, Nikto, SELinux, and AppArmor, this practical course equips diploma students with the skills demanded by the cybersecurity industry and prepares them for higher studies or entry-level security roles in Ethical Hacking, Penetration Testing, Digital Forensics, and Incident Response.

Course Outcome:
After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
01	Set up and navigate the Kali Linux environment and identify its pre-installed cybersecurity tool categories.	Apply
02	Manage files, directories, users, groups, and permissions effectively in a Linux security context.	Apply
03	Monitor and control Linux processes and packages to maintain a secure system environment.	Apply
04	Analyse network traffic and apply essential security tools for threat detection and reconnaissance.	Apply
05	Develop Bash scripts and automation tasks and implement Linux system hardening techniques using UFW, Fail2Ban, SELinux, and AppArmor.	Apply

**Revised Bloom's Taxonomy (RBT)*

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering
Level: Diploma
Branch: Cyber System and Information Security
Subject Code: DI03066011
Subject Name: Linux for Security

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA(M)	PA(I)	ESE (V)	
0	1	4	3	00	00	20	30	50

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1	**Introduction to Kali Linux and Cybersecurity Lab Environment** **Introduction to Kali Linux:** purpose, history, and comparison with Ubuntu and Parrot OS **Kali Linux variants:** Full Install, Live Boot, Kali NetHunter (mobile), Kali on WSL **Lab environment setup:** installing Kali Linux and Ubuntu on VirtualBox/VMware; configuring NAT, Bridged, and Host-only network modes. Managing Kali packages- apt update, apt upgrade, apt install; verifying tool integrity using checksums and GPG signatures	06	10
2	File System Management and Navigation File and Directory Management: mkdir, touch, nano, cat, less, more, head, tail, creating, copying, moving, renaming and deleting files and directories Linux File System Hierarchy and Navigation: /etc, /var, /home, /usr, /proc, /dev, Hard links and symbolic links- ln, ln -s, Searching files- find, locate, which, whereis Text processing for security: grep, awk, sed, cut, sort, uniq	08	15

3	User, Group Management and File Permissions User and Group Management: adduser, useradd, usermod, userdel, passwd, chage, Group Management- groupadd, groupmod, groupdel, gpasswd, id, groups, /etc/passwd, /etc/shadow, /etc/group file structure and security implications File Permissions and Ownership: chmod (symbolic & numeric), chown, chgrp, Default permissions and umask configuration, Special permission bits- SUID, SGID, Access Control Lists (ACLs)- setfacl, getfacl for granular access control, Sudo configuration: /etc/sudoers, principle of least privilege	10	15
4	Process Management and Package Management Process Management: ps, top, htop, pgrep, kill, killall, nice, renice, jobs, bg, fg, nohup, understanding process hierarchy and zombie/orphan processes, Security perspective- identifying malicious processes and suspicious PIDs Package Management on Debian/Ubuntu: apt, dpkg, apt-cache, apt-get, Verifying package integrity- checksums, GPG signatures	08	15
5	**Networking, Network Commands and Essential Security Tools** **Networking Basics:** IP addressing, DNS, Gateway, subnetting fundamentals, netplan, /etc/network/interfaces, nmcli, ping, traceroute, nslookup, dig, host, netstat, ss, lsof -i – identifying open ports, ifconfig, ip addr, ip route, ip link **Network Reconnaissance and Packet Analysis Tools:** SYN scan, UDP scan, OS & service detection, whois – gathering target information, tcpdump – filters, saving and reading pcap files, Netcat (nc)- banner grabbing, port testing, simple file transfer	14	20

6	Linux Security Automation, Log Monitoring, and System Hardening Bash Scripting Fundamentals: variables, data types, read, echo, printf, Control structures: if-else, case, while, for, until loops, Functions, arguments, exit codes and error handling in scripts Automation with Bash: writing practical security automation scripts, Crontab jobs: crontab -e, cron.d, cron.daily System Logs and Monitoring: /var/log/syslog, auth.log, kern.log, dmesg, journalctl, logrotate, last, lastb, who, w, Parsing logs with grep, awk, and sed Linux System Hardening: UFW – rules, profiles, enable/disable, Fail2Ban: configuration, jails, banning IPs, monitoring logs, SELinux: modes (enforcing, permissive, disabled), contexts, audit2allow, AppArmor: profiles, aa-status, aa-enforce, aa-complain, SSH hardening: key-based auth, disabling root login, port change	14	25
	Total	**60**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
0	**0**	**0**	**0**	**0**	**0**

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. The Linux Command Line, William E. Shotts, No Starch Press, 2019, 978-1-59327-955-4
2. Linux Basics for Hackers, OccupyTheWeb, No Starch Press, 2018, 978-1-59327-855-7
3. Linux Security Cookbook, Daniel J. Barrett et al., O'Reilly Media, 2003, 978-0-596-00391-0
4. Penetration Testing, Georgia Weidman, No Starch Press, 2014, 978-1-59327-564-8
5. Hacking: The Art of Exploitation, Jon Erickson, No Starch Press, 2nd Ed., 2008, 978-1-59327-144-2
6. The Practice of Network Security Monitoring, Richard Bejtlich, No Starch Press, 2013, 978-1-59327-509-9

(b) Open source software and website:

1. Linux Journey – Interactive Linux learning platform: https://linuxjourney.com/
2. OverTheWire – Wargames for Linux security (Bandit, Narnia): https://overthewire.org/wargames/
3. TryHackMe – Guided cybersecurity labs: https://tryhackme.com/
4. Hack The Box – Penetration testing practice labs: https://www.hackthebox.com/
5. Kali Linux Documentation – Official tool reference: https://www.kali.org/docs/
6. Nmap Official Documentation: https://nmap.org/
7. Wireshark Documentation: https://www.wireshark.org/docs/
8. OWASP Foundation – Security guidelines and checklists: https://owasp.org/
9. GeeksforGeeks – Linux security tutorials: https://www.geeksforgeeks.org/linux-security/
10. NVD – National Vulnerability Database (CVE lookup): https://nvd.nist.gov/
11. CIS Benchmarks – Linux hardening standards: https://www.cisecurity.org/cis-benchmarks
12. Aircrack-ng Documentation: https://www.aircrack-ng.org/documentation.html

Suggested Course Practical List:

Practical 1: Linux Security Lab Environment Setup

Install VirtualBox/VMware and create a cybersecurity lab by installing Kali Linux, Ubuntu, and Metasploitable2 virtual machines. Configure NAT, Bridged, and Host-only networking, update Kali repositories using apt update and apt upgrade, and verify connectivity between VMs.

Practical 2: Linux File System Navigation and File Operations

Practice file and directory operations using mkdir, touch, cp, mv, rm, nano, cat, less, head, and tail. Explore Linux directory structure (/etc, /var, /home, /usr) and create hard and symbolic links using ln and ln -s.

Practical 3: Searching and Text Processing

Search files using find, locate, which, and whereis. Perform text processing for security analysis using grep, awk, sed, cut, sort, and uniq.

Practical 4: User and Group Security Management

Create, modify, and delete users and groups using useradd, usermod, userdel, passwd, groupadd, and groupdel. Analyze /etc/passwd, /etc/shadow, and /etc/group, and configure password policies using chage.

Practical 5: File Permissions and Access Control

Manage file permissions using chmod, chown, and chgrp. Demonstrate SUID, SGID, and Sticky Bit usage. Implement Access Control Lists (ACLs) using setfacl and getfacl, and configure secure sudo privileges using visudo.

Practical 6: Process Monitoring and Management

Monitor system processes using ps, top, htop, and pgrep. Manage processes using kill, killall, nice, renice, jobs, bg, and fg. Identify suspicious or high-resource processes from a security perspective.

Practical 7: Package Management and Verification

Install and manage software packages using apt, dpkg, apt-cache, and apt-get. Verify package authenticity using checksums and GPG signatures.

Practical 8: Network Configuration and Monitoring

Configure network interfaces using ip addr, ip route, and ip link. Test connectivity using ping, traceroute, nslookup, dig, and host. Identify open ports and services using netstat, ss, and lsof.

Practical 9: Information Gathering and Reconnaissance

Perform passive reconnaissance using whois, dig, nslookup, and host. Use tools such as theHarvester, dnsenum, and fierce to gather domain and DNS information.

Practical 10: Network Scanning using Nmap

Perform network scanning using Nmap, including TCP connect scan (-sT), SYN scan (-sS), UDP scan (-sU), service detection (-sV), OS detection (-O), and subnet scanning.

Practical 11: Packet Capture and Analysis

Capture and analyze network traffic using tcpdump and Wireshark. Apply capture and display filters, follow TCP streams, and analyze HTTP and DNS traffic.

Practical 12: Netcat for Network Testing

Use Netcat (nc) for banner grabbing, port testing, and simple file transfer between virtual machines.

Practical 13: Bash Scripting for Security Automation

Write Bash scripts using variables, loops, and conditional statements to automate security tasks such as detecting failed SSH logins, auditing file permissions, and monitoring system activity. Schedule scripts using crontab.

Practical 14: System Logs Monitoring and Rootkit Detection

Analyze system logs such as /var/log/syslog, /var/log/auth.log, and kern.log. Use tools like journalctl, last, lastb, and who. Detect suspicious login attempts and scan for rootkits using chkrootkit and rkhunter.

Practical 15: Linux Firewall and System Hardening

Configure UFW firewall rules, restrict SSH access, and enable rate limiting. Configure Fail2Ban to block brute-force attacks. Implement SSH hardening (disable root login, enable key-based authentication) and review SELinux/AppArmor security profiles. Harden SSH: disable root login, enable key-based auth, change default port.

List of Laboratory/Learning Resources Required:

1. Computer System Configuration:

Sr.	Specification
1.	Processor: Intel Core i5 or equivalent and above
2.	RAM: 8 GB minimum (16 GB recommended for running multiple virtual machines)
3.	Storage: 256 GB SSD / HDD minimum
4.	Operating System: Ubuntu Linux 22.04 LTS or Kali Linux 2024 (pre-installed or VM)
5.	Virtualization: VT-x / AMD-V enabled in BIOS for running Metasploitable2 VM
6.	Wireless Network Adapter: USB wireless adapter supporting monitor mode (for wireless security labs)

2. Software Requirements:

Tool / Software	Purpose in Course	Download URL
Ubuntu / Kali Linux	Primary OS for all practical sessions	ubuntu.com / kali.org
VirtualBox / VMware	Virtualisation platform for isolated lab environments	virtualbox.org
Metasploitable2	Intentionally vulnerable target VM for scanning and testing	sourceforge.net
Nmap	Network scanner for port and service enumeration	nmap.org
Wireshark / tcpdump	Packet capture and network traffic analysis	wireshark.org
Netcat (nc)	Port testing, banner grabbing, simple file transfer	Built-in on most Linux distros
Hydra	Password attack tool (lab use only)	Built-in on Kali Linux
Nikto	Web vulnerability scanner	Built-in on Kali Linux

UFW	Uncomplicated Firewall for rule-based traffic control	Built-in on Ubuntu Linux
Fail2Ban	Automated IP banning for brute-force protection	fail2ban.org
SELinux / AppArmor	Mandatory access control for system hardening	Built-in on RHEL / Ubuntu
chkrootkit / rkhunter	Rootkit and malware detection tools	Built-in on Kali Linux
Whois / Dig / Nslookup	Domain reconnaissance and DNS analysis	Built-in on most Linux distros
Aircrack-ng	Wireless network security analysis (lab use only)	aircrack-ng.org

Suggested Project List:

Sr.	Project Title	Description
1.	**Linux Permission Audit Tool (Bash + Python)**	Develop a script that scans a Linux system for misconfigured file permissions, world-writable files, SUID/SGID binaries, and weak sudo rules. Generate a colour-coded HTML audit report with recommended fixes.
2.	**Automated User Account Security Manager (Bash)**	Build a Bash-based tool that enforces password policy, disables inactive accounts, verifies /etc/shadow integrity, and generates a user account health report for system administrators.
3.	**Network Recon and Port Scan Automation (Nmap + Bash)**	Write a Bash wrapper around Nmap to automate scheduled network scans, compare results over time, detect newly opened ports, and send alert summaries to a log file.
4.	**Live Traffic Anomaly Detector (tcpdump + Python)**	Capture network traffic using tcpdump, parse the output with Python, and flag anomalous connections (unexpected IPs, unusual port activity, high packet rates). Display results in a real-time terminal dashboard.

5.	**Linux System Hardening Checklist Implementer (Bash)**	Automate the application of a CIS-benchmark-inspired hardening checklist: configure UFW rules, enable Fail2Ban, disable unused services, harden SSH, and produce a before/after security posture comparison report.
6.	**Log Analysis and Threat Intelligence Dashboard (Python)**	Parse /var/log/auth.log, syslog, and journalctl output using Python. Identify brute-force attempts, privilege escalations, and suspicious commands. Display an interactive terminal dashboard using curses or a simple HTML report.
7.	**Cron-Based Security Monitoring System (Bash + Crontab)**	Design a scheduled monitoring system using crontab that periodically checks for failed logins, new user accounts, changed SUID binaries, and modified system files, then logs findings and sends file-based alerts.
8.	**Multi-Layer Hardened Web Server Deployment (Apache + UFW + Fail2Ban)**	Deploy an Apache web server on Ubuntu with full security hardening: TLS configuration, UFW firewall rules, Fail2Ban for HTTP protection, AppArmor profile enforcement, and Nikto scan verification of security posture.
9.	**Wireless Security Audit Tool (Python + Scapy)**	Develop a Python-based tool using Scapy to passively scan for wireless networks, detect open or WEP-protected networks, and generate a security risk report with recommendations for mitigation.

Suggested Activities for Students:

In addition to laboratory sessions, students are encouraged to participate in the following co-curricular and experiential learning activities to strengthen practical security skills, promote ethical thinking, and enhance employability in the cybersecurity domain.

a) Hands-on Lab Exploration in a Controlled Virtual Environment

- Set up a personal virtual lab with VirtualBox, Kali Linux, and Metasploitable2 for safe practice.
- Practice Linux hardening techniques, process monitoring, and log analysis in an isolated environment — never on production systems.

b) Participation in Capture The Flag (CTF) Competitions

- Participate in beginner-friendly CTF platforms such as PicoCTF, OverTheWire (Bandit), and TryHackMe Linux rooms.
- Develop problem-solving skills in file permissions, bash scripting, privilege escalation, and network forensics.

c) Bash Script Development and Sharing

- Write and share security-automation Bash scripts on GitHub as a personal portfolio.

- Participate in open-source projects related to Linux security tools to gain collaborative development experience.

d) Vulnerability Research and CVE Study

- Study published CVEs related to Linux (kernel vulnerabilities, sudo exploits, misconfiguration risks) from NVD.
- Analyse how proper hardening (covered in Unit 5) could have prevented each documented vulnerability.

e) Study and Presentation of Real-World Security Incidents

- Analyse real incidents involving Linux servers (e.g., Shellshock, Dirty COW, Log4Shell) and present root causes.
- Discuss how specific techniques from this course — hardening, log analysis, firewall rules — could have mitigated each incident.

f) Online Certifications and MOOCs

- Students are encouraged to register for cybersecurity courses on platforms such as TryHackMe, Hack The Box Academy, Coursera, and NPTEL.
- Relevant courses: Linux Fundamentals, Introduction to Cybersecurity, Network Security Basics.

****