QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**		
Course No.	**0133213**		**Course name**		Infrastructure Security Using Linux		
Credit Hours	**3**		**Prerequisite Co-requisite**		Applied Programming 0130231		
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements**	☐ Elective requirements	
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓Traditional learning		
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 face to face : 1synchronous		☐ ✓**3 Traditional**		

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Dr Hani al Mimi	**assistant professor**	**226**			
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

The students will have knowledge in underlying operating systems environments such as Linux and Windows and how they contribute, as hosts, to the success of many other applications like network operations and data centers. Students will gain the skills needed to protect Unix and Linux servers from various types of threats. They will learn how to manage users, groups, permissions, ownership, storage, files, directories, Linux boot process, system components, devices, networking, packages, and software.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	Linux Basics For Hackers_ Getting Started With Networking, Scripting, And Security In Kali 2018
Supportive learning resources (Books, databases, periodicals, software, applications, others)	**1.** Richard Blum, Christine Bresnahan - CompTIA Linux+ Study Guide_ Exam XK0-005 (2022, Sybex) - libgen.li **2.** Christine Bresnahan and Richard Blum, CompTIA Linux+ Study Guide, John Wiley & Sons, Inc., 4rd ed., 2019. **3.** Karnel Erickson, Cyber security: Kali Linux for hackers and Hacker Basic Security, 2019. 4. Jason Nufryk and Damon Garn,The Official CompTIA Linux+ Student Guide, CompTIA, first edition, 2019.
Supporting websites	https://linuxjourney.com/ https://overthewire.org/wargames/

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

The physical environment for teaching	☐ **Class room**	☐ ✓labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Introducing Linux operating system philosophy	**1**
K2	Describes Users, Groups, Permissions and Ownership in Linux, Linux processes	**2**
K3	Introducing the Devices, Networking, Packages, and Software in Linux.	**2**
	Skills	
S1	Applying and exploring shell commands of Linux operating system.	**6**
S2	Managing the users, groups, permissions, ownership, storage, files, directories, kernel modules, Linux boot process, system components, devices, networking, and packages & software in Linux.	**6**
	Competences	
C1	Make judgments with regards to relevant scientific, societal, and ethical aspects, and testing & decide with the working team whether a given Linux system configuration is secure or not.	**12**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction, Performing Basic Linux Tasks	Face to Face on lab	Linux Basics For Hackers
2	Managing Users, Managing Groups	Face to Face on lab	Linux Basics For Hackers
3	Managing Permissions – part 1, Managing Permissions – practical	Face to Face on lab	Linux Basics For Hackers
4	Managing Ownership – part 1, Managing Ownership – practical	Face to Face on lab	Linux Basics For Hackers
5	Managing Storage, Managing file system	Face to Face on lab	Linux Basics For Hackers
6	Managing Files and Directories, Managing Files and Directories – practical	Face to Face on lab	Linux Basics For Hackers
7	Managing Kernel Modules , Managing Kernel Modules – part 2	Face to Face on lab	Linux Basics For Hackers
8	**Midterm Exam**		
9	Managing the Linux Boot Process – part 1, Managing the Linux Boot Process – part 2	Face to Face on lab	Linux Basics For Hackers
10	Managing System Components, Managing System Components – part 2	Face to Face on lab	Linux Basics For Hackers
11	Managing Devices, Managing Devices – part 2	Face to Face on lab	Linux Basics For Hackers
12	Managing Networking, Managing Networking – part 2	Face to Face on lab	Linux Basics For Hackers
13	Managing Networking, Managing Networking – part 2	Face to Face on lab	Linux Basics For Hackers
14	Managing Packages and Software, Managing Packages and Software – part 2	Face to Face on lab	Linux Basics For Hackers
15			
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

This activities was designed using the Project-Based Learning (PBL)

Project: Linux Boot, System Components & Devices (PBL)

Task / Activity	Reference	Expected Results
Analyze and document Linux boot process stages	Managing the Linux Boot Process – Part 1	Clear understanding of boot sequence
Configure and troubleshoot bootloader settings	Managing the Linux Boot Process – Part 2	Stable boot environment
Identify critical system components and services	Managing System Components – Part 1	Listed and explained components
Configure and manage system services	Managing System Components – Part 2	Running and controlled services
Identify connected hardware devices	Managing Devices – Part 1	Device inventory report
Configure device permissions and drivers	Managing Devices – Part 2	Properly functioning device setup
Test boot stability and system functionality	Related Labs & Practical Activities	Fully functional Linux system
Prepare final documentation	PBL Documentation	Structured technical project report

Week	Task / activity	Reference	Expected results
1	**Introduction, Performing Basic Linux Tasks**	"Linux Basics for Hackers" (Ch. 1-2)	Students understand basic Linux commands, navigate the file system, and perform simple file operations.
2	**Managing Users, Managing Groups**	"Linux Basics for Hackers" (Ch. 3)	Students create and manage users and groups, understand user roles, and set basic group permissions.
3	**Managing Permissions – part 1, Managing Permissions – practical**	"Linux Basics for Hackers" (Ch. 4)	Students gain hands-on experience with file permissions (chmod, chown) and configure access control effectively.
4	**Managing Ownership – part 1, Managing Ownership – practical**	"Linux Basics for Hackers" (Ch. 4)	Students assign and modify ownership of files

			and directories, understanding user, group, and other concepts.
5	**Managing Storage, Managing File System**	"Linux Basics for Hackers" (Ch. 5)	Students partition, format, and mount storage devices, understanding file system hierarchy and management.
6	**Managing Files and Directories, Managing Files and Directories – practical**	"Linux Basics for Hackers" (Ch. 6)	Students perform practical tasks like creating, deleting, moving, and finding files using Linux commands.
7	**Managing Kernel Modules, Managing Kernel Modules – part 2**	"Linux Basics for Hackers" (Ch. 7)	Students learn to manage kernel modules (lsmod, modprobe), loading/unloading modules as needed.
8	**Managing the Linux Boot Process – part 1, part 2**	"Linux Basics for Hackers" (Ch. 8)	Students understand GRUB, system initialization processes, and troubleshoot common boot issues.
9	**Managing System Components, Managing System Components – part 2**	"Linux Basics for Hackers" (Ch. 9)	Students configure and manage system processes, services, and daemons (systemctl, service).
10	**Managing Devices, Managing Devices – part 2**	"Linux Basics for Hackers" (Ch. 10)	Students interact with hardware devices, manage drivers, and understand device file management (/dev).
11	**Managing Networking, Managing Networking – part 2**	"Linux Basics for Hackers" (Ch. 11-12)	Students configure IP addresses, use basic network tools (ping, ifconfig, netstat), and test connectivity.
12	**Managing Packages and Software, Managing Packages and Software – part 2**	"Linux Basics for Hackers" (Ch. 13)	Students install, update, and remove software packages using package managers (apt, dpkg).
13	**Introduction, Performing Basic Linux Tasks**	"Linux Basics for Hackers" (Ch. 1-2)	Students understand basic Linux commands, navigate the file system,

			and perform simple file operations.