F01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**	
Course No.	**0133308**		**Course name**		**Cybersecurity Tools and Techniques**	
Credit Hours	**3**		**Prerequisite Co-requisite**		Programming for Cyber Security - 0133333	
Course type	☐ MANDATORY UNIVERSITY Requirement	☐ University elective Requirement	☐ FACULTY MANDATORY Requirement	☐ Support course family requirements	☐ Mandatory requirement	☐ ✓ **Elective requirements**
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓ Traditional learning	
Teaching model	☐ Synchronous:1asynchronous		☐✓ 2 face to face: synchronous		☐ 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	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course provides a practical, hands-on examination of the fundamental tools and techniques used by cybersecurity professionals to protect, defend, and assess the security posture of information systems. Moving beyond theoretical concepts, students will learn *how* to apply industry-standard software to real-world scenarios in a controlled laboratory environment.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	*CompTIA Security+ Guide to Network Security Fundamentals* **Author:** Mark Ciampa **Publisher:** Cengage Learning
Supportive learning resources (Books, databases, periodicals, software, applications, others)	*Hands-On Ethical Hacking and Network Defense* **Authors:** Michael Simpson, Nicholas Antill **Publisher:** Cengage Learning
Supporting websites	

F01/0408-4.0E	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**			

Security Department

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Knowledge of the cybersecurity lifecycle, including reconnaissance, scanning, exploitation, and maintaining access.	MK1
K2	Knowledge of legal and ethical frameworks (Rules of Engagement) and compliance standards regarding security testing.	MK2
K3	Knowledge of network protocols (TCP/IP) and how they are manipulated or analyzed by security tools.	MK3
K4	Knowledge of vulnerability management methodologies and the Common Vulnerability Scoring System (CVSS).	MK4
K5	Knowledge of different types of security tools (Open Source vs. Commercial) and their specific use cases.	MK5
K1	Knowledge of the cybersecurity lifecycle, including reconnaissance, scanning, exploitation, and maintaining access.	MK1
	Skills	
S1	Applying network reconnaissance and enumeration tools (e.g., Nmap) to identify active hosts and services.	MS1
S2	Applying vulnerability scanning tools (e.g., Nessus, OpenVAS) to detect and classify system flaws.	MS2
S3	Applying packet sniffing and analysis tools (e.g., Wireshark) to interpret network traffic and detect anomalies.	MS3
S4	Applying exploitation frameworks (e.g., Metasploit) to validate vulnerabilities in a controlled lab environment.	MS4
	Competences	
C1	Conducting a comprehensive security assessment independently using appropriate tools and techniques.	MC1

C2	Discussing and reporting technical security findings and mitigation strategies to both technical and management audiences.	MC2

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 to Cybersecurity Tools: Ethics, Legal Issues (RoE), and the Security Lifecycle	Lecture	Ref 1, Ref 2
2	Lab Environment Setup: Virtualization (VirtualBox/VMware), Kali Linux Introduction, and Command Line Basics	Lab / Workshop	Ref 2
3	Reconnaissance (Passive): OSINT, Footprinting, Search Engines (Shodan), and DNS Interrogation	Lecture / Lab	Ref 2
4	Reconnaissance (Active): Network Scanning, Port Scanning (TCP/UDP), and OS Fingerprinting (Nmap)	Lab	Ref 2
5	Enumeration: Extracting Usernames, Group Details, and Shares (NetBIOS, SNMP, LDAP)	Lab	Ref 2
6	Vulnerability Assessment: Automated Scanners (Nessus/OpenVAS) and CVSS Scoring	Lecture / Lab	Ref 1, Ref 2

7	Network Sniffing & Traffic Analysis: Packet Capture, Filtering, and Inspection (Wireshark, TCPdump)	Lab	Ref 1, Ref 2
8	Midterm Exam (30%)	Exam	--
9	Password Attacks: Hashing, Cracking Tools (John the Ripper, Hashcat), and Brute Force defense	Lab	Ref 2
10	Exploitation Frameworks: Introduction to Metasploit, Payloads, Shells, and Meterpreter	Lab	Ref 2
11	Web Application Security: SQL Injection, XSS, and Web Proxies (Burp Suite)	Lecture / Lab	Ref 2
12	Wireless Network Security: Wi-Fi Tools, WPA2/WPA3 Cracking, and Signal Analysis (Aircrack-ng)	Lab	Ref 1
13	Defensive Tools (Blue Team): Configuring Host-Based Firewalls (iptables) and IDS/IPS basics (Snort)	Lecture / Lab	Ref 1
14	Forensics & Incident Response: Disk Imaging, Log Analysis, and Integrity Checking (File Hashes)	Lecture / Lab	Ref 1
15	Practical Projects Discussion & Lab Final	Discussion / Presentation	--
16	Final Exam	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)

Week	Task / activity	Reference	Expected results
1	Lecture: Reviewing Legal Agreements & Rules of Engagement (RoE).	Ref 1, Ref 2	Students can draft a sample scope-of-work and identify legal boundaries for testing.
2	Lab: Installing Kali Linux and setting up the Virtual Lab (VirtualBox/VMware).	Ref 2	A fully functional virtual environment with attacker and victim machines ready for use.
3	Lab: Performing Passive Reconnaissance using OSINT tools (TheHarvester, Shodan).	Ref 2	A preliminary intelligence report listing target

			domain details without touching the target network.
4	Lab: Active Network Scanning using Nmap (Ping sweeps, SYN scans).	Ref 2	A network topology map identifying active live hosts and their IP addresses.
5	Lab: Service Enumeration (NetBIOS, SNMP) to identify users and shares.	Ref 2	A list of open ports, running service versions, and potential usernames extracted from the target.
6	Lab: Running Automated Vulnerability Scans using Nessus or OpenVAS.	Ref 1, Ref 2	A generated Vulnerability Assessment Report classified by severity (High/Medium/Low).
7	Lab: Packet Sniffing and Traffic Analysis using Wireshark.	Ref 1, Ref 2	Capturing a PCAP file and successfully filtering it to read clear-text credentials (e.g., Telnet/FTP).
8	Midterm Exam	--	Assessment of theoretical knowledge and basic tool usage (Weeks 1-7).
9	Lab: Password Auditing and Cracking using John the Ripper and Hashcat.	Ref 2	Successfully recovering a plaintext password from a provided hash file.
10	Lab: Exploitation using Metasploit Framework (MSF).	Ref 2	Establishing a remote shell (Meterpreter session) on a vulnerable target machine.
11	Lab: Web Application Analysis using Burp Suite (Proxy usage).	Ref 2	Intercepting HTTP requests and modifying parameters to test for SQL Injection or XSS.
12	Lab: Wireless Security Assessment (Aircrack-ng suite).	Ref 1	Capturing a WPA/WPA2 4-way handshake for offline analysis.
13	Lab: Blue Team Defense - Configuring iptables and IDS rules (Snort).	Ref 1	A hardened Linux system with specific firewall rules that block the attacks

			learned in previous weeks.
14	Lab: Digital Forensics basics (Hashing and Log Analysis).	Ref 1	Verifying file integrity using MD5/SHA sums and identifying attack signatures in system logs.
15	Project Presentation: Conducting a mini-Penetration Test on a test server.	All Refs	A comprehensive final report detailing discovered vulnerabilities and recommended fixes.
16	Final Exam	--	Comprehensive assessment of all course learning outcomes.