KINGDOM OF SAUDI ARABIA
Technical and Vocational Training Corporation
General Directorate of Curricula

المملكة العربية السعودية
المؤسسة العامة للتدريب التقني والمهني
الإدارة العامة للمناهج

الخطط التدريبية للكليات التقنية

Training Plans for Technical Colleges

CURRICULUM FOR Department

Engineering of Computer and Information Technology

Major
Cyber Security

نسخة أولية (تحت المراجعة)

Under Revision Draft

A Bachelor's Degree

Index

Program Description

The Cybersecurity Program gives the trainee a deep understanding and practical skills in state of the art of Cybersecurity. It includes but not limited to multiple areas such as Operating Systems security, networks & communications security, Securing Software Development, and Cloud Computing & Virtualization security. The students will acquire skills to be assessed also in Digital forensics, Penetration Testing, Risk Management & Incident Response, Information Security Management, and Advanced Security Topics.

The program aims to achieve the following objectives:

- Understand the major state of the art concepts in Cyberspace security.
- Mastering the skills of securing wired and wireless networks & communications.
- Mastering the skills of building secure electronic systems and services.
- Mastering different methods of security penetration testing for systems and networks.
- Explore different technologies and applications in digital data encryption
- Increase the level of analytical capacity and investigation of incidents and digital crimes.
- Mastering risk management skills in information security departments.

Admission Requirements: The applicant must have a diploma in one of the following: Computer Networks, Computer Network Systems Administration, Technical Support, Computer Programming or Telecommunications.

The Curriculum Framework Distributed on Trimesters توزيع الخطة التدريبية على الفصول التدريبية لمرحلة البكالوريوس بالنظام الثلثي

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
1st Trimester	1	ENGL 301	English Language (1)		4	4	0	2	6		لغة انجليزية ١	٣٠١ انجل	١	الفصل التدريبي الأول
	2	MATH 304	Applide Mathematics		4	3	2	1	6		رياضيات تطبيقية	٣٠٤ رياض	٢	
	3	INSA 312	Basic Networks Systems Administration		5	2	6	0	8		أساسيات إدارة أنظمة الشبكات	٣١٢ نشبك	٣	
	4	INET 313	Computer Networks		6	4	4	0	8		شبكات الحاسب	٣١٣ شبكا	٤	
	Total Number of Units				19	13	12	3	28	المجموع				

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
2nd Trimester	1	ENGL302	English Language (2)	ENGL 301	4	4	0	2	6	٣٠١ انجل	لغة انجليزية ٢	٣٠٢ انجل	١	الفصل التدريبي الثاني
	2	INSA 444	Open Source Network Systems	INSA 312	4	3	2	0	5	٣١٢ نشبك	أنظمة شبكات المصادر المفتوحة	٤٤٤ نشبك	٢	
	3	CYBR 321	Fundamentals of Cyber Security		3	2	2	0	4		أساسيات الأمن السيبراني	٣٢١ سيبر	٣	
	4	CYBR 351	Foundation of Computer Programming		4	2	4	0	6		مبادئ برمجة الحاسب	٣٥١ سيبر	٤	
	Total Number of Units				15	11	8	2	21	المجموع				

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
3rd Trimester	1	STAT 303	Statistics and Probability		3	3	0	1	4		الإحصاء والإحتمالات	٣٠٣ احصا	١	الفصل التدريبي الثالث
	2	GNRL 402	Engineering Project Management		3	3	0	1	4		إدارة المشاريع الهندسية	٤٠٢عامة	٢	
	3	CYBR 312	Operating Systems Security	INSA 312 CYBR 321	4	2	4	0	6	٣١٢ نشبك ٣٢١ سيبر	أمن أنظمة التشغيل	٣١٢ سيبر	٣	
	4	CYBR 322	Applied Cryptography	MATH 304 CYBR 321	3	3	0	0	3	٣٠٤ رياض ٣٢١ سيبر	التشفير التطبيقي	٣٢٢ سيبر	٤	
	5	CYBR 352	Advanced programming	CYBR 351	4	2	4	0	6	٣٥١ سيبر	برمجة متقدمة	٣٥٢ سيبر	٥	
	Total Number of Units				17	13	8	2	23	المجموع				

CRH: Credit Hours L: Lecture P: Practical T: Tutorial CTH: Contact Hours

و.م : وحدات معتمدة، مح : محاضرة، عم : عملي/ ورش، تم : تمارين، س.أ : ساعات اتصال أسبوعي

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
4th Trimester	1	GNRL405	Engineering Economy		3	3	0	1	4		إقتصاد هندسي	٤٠٥ عامة	١	الفصل التدريبي الرابع
	2	CYBR 441	Networks & Communications Security	INET 313 CYBR 322	4	2	4	0	6	٣١٣ شبكا ٣٢٢ سيبر	أمن الشبكات والاتصالات	٤٤١ سيبر	٢	
	3	CYBR 444	Cloud Computing & Virtualization Security	CYBR 312 INSA 444	4	2	4	0	6	٣١٢ سيبر ٤٤٤ نشبك	أمن الحوسبة السحابية و الأنظمة التخيلية	٤٤٤ سيبر	٣	
	4	CYBR 453	Secure Software development	CYBR 352	4	2	4	0	6	٣٥٢ سيبر	تأمين تطوير البرمجيات	٤٥٣ سيبر	٤	
	Total Number of Units				15	9	12	1	22	المجموع				

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
5th Trimester	1	CYBR 423	Penetration Testing	CYBR 453	4	2	4	0	6	٤٥٣ سيبر	اختبار الاختراق	٤٢٣ سيبر	١	الفصل التدريبي الخامس
	2	CYBR 431	Information Security Management	CYBR 444 CYBR 453	3	2	2	0	4	٤٤٤ سيبر ٤٥٣ سيبر	إدارة أمن المعلومات	٤٣١ سيبر	٢	
	3	CYBR 442	Advanced Technologies in Networks Security	CYBR 441	4	2	4	0	6	٤٤١ سيبر	التقنيات المتقدمة في أمن الشبكات	٤٤٢ سيبر	٣	
	4	CYBR 443	Wireless Networks Security	CYBR 441	3	2	2	0	4	٤٤١ سيبر	أمن الشبكات اللاسلكية	٤٤٣ سيبر	٤	
	5	CYBR ***	Elective Course -1		3	2	2	0	4		مقرر اختياري - ١	*** سيبر	٥	
	Total Number of Units				17	10	14	0	24	المجموع				

	No.	Course Code	Course Name	Prereq	No. of Units					المتطلب	اسم المقرر	رمز المقرر	م	
					و.م	مح	عم	تم	س.أ					
					CRH	L	P	T	CTH					
6th Trimester	1	CYBR 424	Digital forensics	CYBR 423 CYBR 444	4	2	4	0	6	٤٢٣ سيبر ٤٤٤ سيبر	الفحص الجنائي الرقمي	٤٢٤ سيبر	١	الفصل التدريبي السادس
	2	CYBR 432	Risk Management & Incident Response	CYBR 431	3	2	2	0	4	٤٣١ سيبر	إدارة المخاطر والإستجابة للحوداث	٤٣٢ سيبر	٢	
	3	CYBR 461	Ethics and Cyber Law	CYBR 423	2	2	0	0	2	٤٢٣ سيبر	الأخلاقيات و قانون الأمن السيبراني	٤٦١ سيبر	٣	
	4	CYBR ***	Elective Course-2		3	2	2	0	4		مقرر اختياري - ٢	***سيبر	٤	
	5	CYBR 491	Graduation Project	CYBR 423 CYBR 431 CYBR 442	4	2	4	0	6	٤٢٣ سيبر ٤٣١ سيبر ٤٤٢ سيبر	مشروع التخرج	٤٩١ سيبر	٥	
	Total Number of Units				16	10	12	0	22	المجموع				

CRH: Credit Hours L: Lecture P: Practical T: Tutorial CTH: Contact Hours

و.م : وحدات معتمدة، مح : محاضرة، عم : عملي/ورش، تم : تمارين، س.أ : ساعات اتصال أسبوعي

	CRH	L	P	T	CTH	
Total Number of Semesters Units	و.م	مح	عم	تم	س.أ	المجموع الكلي لوحدات البرنامج
	99	66	66	8	140	

Total Contact Hours × 13	Co-operative Training	المجموع الكلي لوحدات التدريب	التدريب التعاوني	ساعات الإتصال الكلية × ١٣
1820	0	1820	٠	١٨٢٠

Elective Courses

	No.	Course Code	Course Name	Prereq	No. of Units و.م CRH	 مح L	 عم P	 تم T	 س.أ CTH	المتطلب	اسم المقرر	رمز المقرر	م	
Elective Courses -1	1	CYBR 471	Trusted Computing	CYBR 322 INSA 444	3	2	2	0	4	سيبر ٣٢٢ نشبك ٤٤٤	الحوسبة الموثوقة	سيبر ٤٧١	١	المقررات الإختيارية - ١
	2	CYBR 472	Embedded Systems Security	CYBR 322 CYBR 352	3	2	2	0	4	سيبر ٣٢٢ سيبر ٣٥٢	أمن الأنظمة المدمجة	سيبر ٤٧٢	٢	
	CRH: Credit Hours L: Lecture P: Practical T: Tutorial CTH: Contact Hours									و.م : وحدات معتمدة، مح : محاضرة، عم : عملي/ ورش، تم : تمارين، س.أ : ساعات اتصال أسبوعي				

	No.	Course Code	Course Name	Prereq	No. of Units و.م CRH	 مح L	 عم P	 تم T	 س.أ CTH	المتطلب	اسم المقرر	رمز المقرر	م	
Elective Courses -2	1	CYBR 481	Internet of Things Security	CYBR 441	3	2	2	0	4	سيبر ٤٤١	أمن إنترنت الأشياء	سيبر ٤٨١	١	المقررات الإختيارية - ٢
	2	CYBR 482	Advanced Security Topics	CYBR 444 CYBR 453	3	2	2	0	4	سيبر ٤٤٤ سيبر ٤٥٣	موضوعات متقدمة في الأمن	سيبر ٤٨٢	٢	
	CRH: Credit Hours L: Lecture P: Practical T: Tutorial CTH: Contact Hours									و.م : وحدات معتمدة، مح : محاضرة، عم : عملي/ ورش، تم : تمارين، س.أ : ساعات اتصال أسبوعي				

Brief Description

Course Name	**Applied Mathematics**	**Course Code**	**MATH304**	**Credit Hours**	**4**
Description	This course is designed for Cyber Security. It introduces students to basic mathematical principles and functions from discrete mathematics that form the foundation for cryptographic and cryptanalysis methods. The course covers five important themes; Mathematical reasoning and mathematical logic and Structures, algorithmic thinking, the concepts and techniques of number theory, modular arithmetic and finite fields.				

Course Name	**Fundamentals of Cyber Security**	**Course Code**	**CYBR321**	**Credit Hours**	**3**
Description	This course provides a basic introduction to all aspects of cyber-security including business, policy, procedures, communications security, network security, security management, legal issues, political issues, and technical issues. From the course, students will become aware of the cybersecurity aspect and gain knowledge of the related security techniques.				

Course Name	**Foundation of Computer Programming**	**Course Code**	**CYBR351**	**Credit Hours**	**4**
Description	The course provides the students with the required skills to write their own applications. thinking like programming is a mandatory skill that any computer related student should master; therefore the course will give students an introduction to algorithms and problem-solving skills. later in the course, students will master the basics of any programming language structure. variables, mathematical operations, conditional controlling components, looping components, arrays, functions, and basic file system operations are all skills a student will learn in this course.				

Course Name	**Operating Systems Security**	**Course Code**	**CYBR312**	**Credit Hours**	**4**
Description	The course of OSs security encompasses many different techniques and methods, which ensure safety from threats and attacks. OSs security module includes different applications and programs to perform required tasks and stop unauthorized interference. From this course, students will learn many ways, including adherence to the following: **1.** Performing regular OS patch updates. **2.** Installing updated antivirus engines and software. **3.** Scrutinizing all incoming and outgoing network traffic through a firewall. **4.** Creating secure accounts with required privileges only (i.e., user management).				

Course Name	Applied Cryptography	Course Code	CYBR322	Credit Hours	3
Description	This course is a comprehensive introduction to modern cryptography and its related standards. The course emphasis on the application and implementation of various techniques for achieving message confidentiality, integrity, authentication, and non-repudiation. Topics include: Symmetric ciphers; Classical encryption techniques; Block ciphers (DES, AES); Block cipher operation; Random bit generation; Stream ciphers; Asymmetric ciphers (RSA, Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Cryptography); Cryptographic data integrity algorithms (Cryptographic hash functions; Message authentication codes; Digital signatures). Key management and distribution.				

Course Name	Advanced Programming	Course Code	CYBR352	Credit Hours	4
Description	This course extends the study of basic programming principles introduced in the Foundation of Computer Programming course (CYBR351). This course covers web-development techniques in client side that use HTML5, CSS, and JavaScript as web development essentials. In addition, students will learn database basics; SQL and Server side programming.				

Course Name	Secure Software Development	Course Code	CYBR453	Credit Hours	4
Description	This course focuses on integrating security in the Software Development Life Cycle (SDLC). It covers the best practices that the software developer needs to avoid opening up their users, customers, and organization to attack at the application layer. In this course, students will learn how to identify and apply security controls in development environments; Assess the effectiveness of software security; Define and apply secure coding guidelines and standards.				

Course Name	Networks & Communications Security	Course Code	CYBR441	Credit Hours	4
Description	This course will cover theory and practice of Telecommunications and Network Security domain which encompasses topics to include: access control to computer network, weakness and security in routers and switches, transport formats and security measures used to maintain the integrity, availability, authentication and confidentiality of the transmitted information over both private and public communication networks. The different standards securities protocols will be studied, discussed and implemented AAA, IPS/IDS, VPN and PKI over Client/Server, routers, firewalls.				

Course Name	Cloud Computing & Virtualization Security	Course Code	CYBR444	Credit Hours	4
Description	This is an introductory course to understand the concepts of Cloud Computing, Virtualization and Computer Networks in general. From this course; students will gain an excellent understanding of basic concepts of Cloud Computing, Virtualization, and Computer Networks. This includes the definitions of CCV, cloud types and cloud service deployment models (IaaS*, PaaS*, SaaS*), learn how to create virtual machines (VM) using Hypervisors (type-2), and understand Computer Networks and IP Addressing. In Addition, students will learn how to protect data stored online from theft, leakage, deletion, and methods of providing cloud security. Also, this course includes the major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, insecure APIs, poor choice of cloud storage providers, and shared technology with countermeasures.				

Course Name	Penetration Testing	Course Code	CYBR 423	Credit Hours	4
Description	This course teaches students to learn the system and network penetration testing, the tools, techniques used to exploit vulnerabilities, and how to defend against attacks. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. This course will also provide the fundamental information associated with each of the methods employed and insecurities identified. In all cases, remedial techniques will be explored. From this course, students will develop an excellent understanding of issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.				

Course Name	Information Security Management	Course Code	CYBR 431	Credit Hours	3
Description	This course covers issues related to administration and management of the security of enterprise information systems and networks. The course includes the following topics: Planning for security and contingencies, security management models, security management practices, governance, and security policy; threat and vulnerability management, incident management, risk management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations. The course will study the principles and tools related to these topics. The course will also cover security standards, evaluation, and certification process.				

Course Name	Advanced Technologies in Networks Security	Course Code	CYBR 442	Credit Hours	4
Description	This course provides students with in-depth study and practice of advanced concepts in applied systems and networking security, including security policies, access controls, authentication mechanisms, IPS, VPN, NGFW and choosing, deploying, supporting and troubleshooting all security devices. The course will discuss emerging networking techniques, inducing software-defined networking (SDN) and network function visualization (NFV). We will also discuss corresponding security issues in SDN and NFV.				

Course Name	**Wireless Networks Security**	**Course Code**	**CYBR 443**	**Credit Hours**	**3**
Description	In a mobile world, the ability to gain network access in a convenient manner, but yet securely, is becoming more and more of a requirement. This course will explore the wireless standards, authentication issues, common configuration models for commercial versus institution installs and analyze the security concerns associated with ad-hoc and standards-based methods of networking. From this course, the student will gain an understanding of wireless networking, protocols, and standards and security issues.				

Course Name	**Digital Forensics**	**Course Code**	**CYBR424**	**Credit Hours**	**4**
Description	Digital forensics involves the investigation of computer-related crimes with the goal of obtaining evidence to be presented in a court of law. In this course, you will learn the principles and techniques for digital forensics investigation and the spectrum of available computer forensics tools. In this course, students will dive into the bits and bytes to conduct computer, network, mobile and social forensic investigations; interpret e-evidence; make inferences; write defensible reports to be used in legal actions; and understand key elements of expert witness testimony. Students will use FTK (Forensic Tool Kit) along with other forensic tools to recover, search, and analyze e-evidence and create reports.				

Course Name	**Risk Management & Incident Response**	**Course Code**	**CYBR432**	**Credit Hours**	**3**
Description	This course examines information security as a risk management problem where the organization identifies information security risks, evaluates those risks, and makes risk mitigation and acceptance decisions given its resource constraints. In this course, students will learn foundational concepts in risk management and incident response and introduce to standard risk management approaches for identifying, analyzing, and responding to risk, as well as the tools and methodologies for metrics to monitor risk management activities. Students will be able to plan for and respond to intruders in an information system. They will be introduced to various types of security incidents and attacks, and learn methods to prevent detect and react to incidents and attacks.				

Course Name	**Ethics and Cyber Law**	**Course Code**	**CYBR461**	**Credit Hours**	**2**
Description	This course covers important ethics that any cyber security specialist should do and understand. In addition, Saudi cyber laws for digital crimes and Internet laws are mandatory knowledge that students should understand and comply with. Privacy and data protection and intellectual property are taught in this course.				

Course Name	**Trusted Computing**	**Course Code**	**CYBR471**	**Credit Hours**	**3**
Description	This course is an introduction to the fundamental technologies behind Trusted Computing, including machine authentication, data protection, attestation, data backup, and system maintenance, etc. This course will also introduce students to the various software resources that exist today to support TPMs (Trusted Platform Modules) and what capabilities they can provide both at an in-depth technical level and in an enterprise context. Students will also learn about how other technologies such as the Dynamic Root of Trust for Measurement (DRTM) and virtualization can both take advantage of TPMs.				

Course Name	**Embedded Systems Security**	**Course Code**	**CYBR472**	**Credit Hours**	**3**
Description	This course covers advanced topics in the emerging technology of embedded system and internet of things developments. designing and programming an embedded system from hardware to build an integrated application are covered in this course. memory management, processing management, storage and file system management and transmission management in a secure fashion are all skills covered in this course.				

Course Name	**Internet of Things Security**	**Course Code**	**CYBR481**	**Credit Hours**	**3**
Description	IoT Security is a course designed to allow students to acquire knowledge on the fundamentals of safeguarding connected devices and networks in IoT. This course aims to introduce the concept of IoT and its impact on our daily lives, to understand the architecture and components of IoT, and to address the challenges and solutions of deploying IoT in our actual life. From this course, students will become aware of the cybersecurity issues raised by IoT and gain knowledge of the related security techniques in the design issue of the IoT.				

Course Name	**Advanced Security Topics**	**Course Code**	**CYBR482**	**Credit Hours**	**3**
Description	This course will cover the most recent topics in cyber security such as Blockchain, Artificial Intelligence, Machine learning, Big data, Cryptocurrency, etc. From this course, students will have an overview of the most recent cyber security topics.				

Courses Detail Description

Department	General Studies	Major	Cyber Security				
Course Name	Applied Mathematics	Course Code	MATH 304				
Prerequisites		Credit Hours CRH	4		CTH		6
			L	3	P	2	T 1

CRH: **Credit Hours** L: **Lecture** P: **Practical** T: **Tutorial** CTH: **Contact Hours**

Course Description:

This course introduces students to basics of mathematical principles and functions from discrete mathematics that form the foundation for cryptographic and cryptanalysis methods. The course covers five important themes; Mathematical reasoning and mathematical logic and Structures, algorithmic thinking, the concepts and techniques of number theory, modular arithmetic and finite fields. These principles and functions will be helpful in understanding symmetric and asymmetric cryptographic methods examined in (Applied Cryptography) Course.

Topics:

- The Foundations of logic and Proofs
- Basics of discrete structures that include sets, permutations, relations, graphs, trees and finite state machines.
- Algorithms.
- The concepts and techniques of Number Theory.
- Finite fields.

Experiments:

References:

- M. Huth and M. Ryan, Logic in Computer Science, 2nd ed, Cambridge university Press, Cambridge, England, 2004
- Handbook of Proof Theory (Studies in Logic and the Foundations of Mathematics 137) 1st Edition, Kindle Edition by S. R. Buss (Editor) 1998
- R. A. Brualdi, Introductory Combinatorics, 5th ed., Prentice-Hall, Englewood Cliffs, NJ,2009
- Kenneth H. Rosen, 7th ed., Discrete Mathematics and its Applications, MC Graw Hill, 2012
- S. Baase and A. Van Gelder, Computer Algorithms: Introduction to Design and Analysis, 3rd ed., Adisson-Wesley, Reading, MA, 1999
- DECODE, Design & Analysis of Algorithms 2015 A Guide for Engineering Students
- Richard Crandall and Carl Pomerance, 2nd ed., Prime Numbers: A Computational Perspective, Springer-Verlag, New York, 2010
- Richard A. Mollin, Fundamental Number Theory with Application 2nd Edition 2008
- Gary L. Mullen, Daniel Panario, Handbook of Finite Fields, 1st Edition 2013
- Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications 1986

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**The Foundations: Logic and Proofs:** • Propositional Logic • Applications of Propositional Logic • Predicates and Quantifiers • Introduction to Proofs • Proof Methods and Strategy	2

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
2	**Basic Structures: Sets, Functions, Sequences, Sums, and Matrices** • Sets • Cardinality of Sets • Set Operations • Functions • Sequences and Summations • Matrices	4
3	**Algorithms:** • Algorithms • The Growth of Functions • Complexity of Algorithms	4
4	**Number Theory:** • Divisibility and Modular Arithmetic • Integer Representations and Algorithms • Primes and Greatest Common Divisors • Tool to compute Bezout coefficients • Solving Congruencies and Applications	8
5	**Finite fields:** • Groups • Rings • Fields • Finite Fields of the Form GF(p) • Polynomial Arithmetic • Finite Fields of the Form $GF(2^n)$	8

Detailed of Practical Contents		
No.	Contents	Hours
1	**The Foundations: Logic and Proofs:** • Propositional logic • Predicates and quantifiers • Rules of inference and introduction to proofs	2
2	**Basic Structures: Sets, Functions, Sequences, Sums, and Matrices** • Sets, set operations and cardinality of sets • Functions, sequences and summations • Matrices	2
3	**Algorithms:** • Algorithms and complexity of algorithms • The Growth of Functions	4
4	**Number Theory:** • Divisibility and Modular Arithmetic • Integer Representations and Algorithms • Primes and Greatest Common Divisors • Bezout coefficients • Solving Congruencies and Applications	6
5	**Finite fields:** • Groups • Rings • Fields • Finite Fields of the Form GF(p) • Polynomial Arithmetic • Finite Fields of the Form GF(2^n)	6

Textbooks	1	M. Huth and M. Ryan, Logic in Computer Science, 2nd ed, Cambridge university Press, Cambridge, England, 2004
	2	Handbook of Proof Theory (Studies in Logic and the Foundations of Mathematics 137) 1st Edition, Kindle Edition by S. R. Buss (Editor) 1998
	3	R. A. Brualdi, Introductory Combinatorics, 5th ed., Prentice-Hall, Englewood Cliffs, NJ,2009
	4	Kenneth H. Rosen, 7th ed., Discrete Mathematics and its Applications, MC Graw Hill, 2012
	5	S. Baase and A. Van Gelder, Computer Algorithms: Introduction to Design and Analysis, 3rd ed., Adisson-Wesley, Reading, MA, 1999
	6	DECODE, Design & Analysis of Algorithms 2015 A Guide for Engineering Students
	7	Richard Crandall and Carl Pomerance, 2nd ed., Prime Numbers: A Computational Perspective, Springer-Verlag, New York, 2010
	8	Richard A. Mollin, Fundamental Number Theory with Application 2nd Edition 2008
	9	Gary L. Mullen, Daniel Panario, Handbook of Finite Fields, 1st Edition 2013
	10	Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications 1986

<table>
<tr><td><b>Department</b></td><td><b>Computer Engineering and Information Technologies</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Fundamentals of Cyber Security</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR321</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"></td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3">3</td><td colspan="2">CTH</td><td>4</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>2</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

This course will provide a basic introduction to all aspects of cyber-security including business, policy, procedures, communications security, network security, security management, legal issues, and technical issues. The course also covers the analytical part of the cyber security domain through which basic analytical skills can be developed for auditing and forensics of a system. From this course, students will become aware of the cybersecurity aspect and gain knowledge of the related security techniques.

Topics:

- Basic concepts of Cyber Security and its wider scope
- Definitions of “Threats” and “Vulnerabilities” and their consequences
- Standards in Cyber Security and their advantages
- Different categories of the system in which cyber security is critical
- Web Application’s vulnerabilities and their security countermeasures
- Mobile Application’s vulnerabilities and their security countermeasures
- Operating System vulnerabilities and their security countermeasures
- Network Security basic concepts
- Tools associated with network security

Experiments:

References:

- Pfleeger, C.P., Security in Computing 5th Edition, Prentice Hall.
- Cryptography and Network Security by William Stalling, 2011

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Chapter 1: Introduction** • Threats, vulnerabilities, and controls • Confidentiality, integrity, and availability • Attackers and attack types; method, opportunity, and motive • Valuing assets	1
2	**Chapter 2: Toolbox: Authentication, Access Control, and Cryptography** • Authentication, capabilities, and limitations • The three bases of authentication: knowledge, characteristics, possessions • Strength of an authentication mechanism • Implementation of access control • Employing encryption • Symmetric and asymmetric encryption • Message digests • Signatures and certificates	2
3	**Chapter 3: Programs and Programming** • Programming oversights: buffer overflows, off-by-one errors, incomplete mediation, Time-of-check to time-of-use errors • Malicious code: viruses, worms, Trojan horses • Developer countermeasures: program development techniques, security principles • Ineffective countermeasures	3
4	**Chapter 4: The Web—User Side** • Attacks against browsers • Attacks against and from web sites • Attacks seeking sensitive data • Attacks through email	2
5	**Chapter 5: Operating Systems** • Object protection: virtualization, sharing • Memory protection: registers, paging, segmentation • Design qualities: modularity, layering, kernelization • Trusted systems: TCB, reference monitor, trusted path, object reuse, evaluation criteria • Rootkits: power, design	4
6	**Chapter 6: Networks** • Vulnerabilities ○ Threats in networks: wiretapping, modification, addressing ○ Wireless networks: interception, association, WEP, WPA ○ Denial of service and distributed denial of service • Protections ○ Cryptography for networks: SSL, IPsec, virtual private networks ○ Firewalls ○ Intrusion detection and protection systems ○ Managing network security, security information, and event management	4

7	**Chapter 7: Databases** • Database terms and concepts • Security requirements: C-I–A; reliability, types of integrity • Access control; sensitive data, disclosure, inference, aggregation • Data mining and big data	4
8	**Chapter 8: Cloud Computing** • What is a cloud service? • Risks to consider when choosing cloud services • Security tools for cloud environments	4
9	**Chapter 9: Management and Incidents** • Security planning • Incident response and business continuity planning • Risk analysis • Handling natural and human-caused disasters	1
10	**Chapter 10: Legal Issues and Ethics** • Protecting programs and data: copyrights, patents, trade secrets • Computer crime statutes and the legal process • Unique characteristics of digital objects • Software quality: Uniform Commercial Code • Ethics: principles and situations to explore	1
Textbook	• Pfleeger, C.P., Security in Computing 5th Edition. • Cryptography and Network Security by William Stalling, 2011	

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**Lab1:** Researching Network Attacks and Security Audit Tools • Research network attacks that have occurred. • Select a network attack and develop a report. • Research network security audit tools. • Select a tool and develop a report	2
2	**Lab 2: Network Monitoring** • Experience Network Monitoring Tools (Solarwind, Wireshark, PRTG, etc.) • Through monitoring tools, • learning how to track network activity, • viewing specific frame, TCP, IP, and HTTP information, • viewing specific packets being sent and received on the network, • viewing information within those packets and spot malicious or suspicious network behavior.	5
3	**Lab 3: Application Threat Analysis** • Testing example of Web applications against threats • Testing example of browsers against threats • Testing example of Mobile applications against threats	3
4	**Lab 4: Coding Practices** • Write the code as per standard practices ○ Client-Server Application in C • Analyze the Vulnerabilities of different languages used • Write the code as per standard practices ○ A webpage having a form • Analyze the Vulnerabilities of different languages used	4
5	**Lab 5: Web Threat Analysis** • Analyze known malicious browser plugins • Analyze phishing techniques using Damn Vulnerable Web App (DVWA) • Devise Security measures against phishing	3
6	**Lab 6: Databases** • Install and run Database Server • Add/remove entries using a webpage • Practice known database attacks • Apply Countermeasures	3
7	**Lab 7: OS Security** • Analyze vulnerabilities of Windows and Linux • Explore system Firewalls	3
8	**Lab 8: Network Security** • Analyze network traffic using Wireshark • Practice known attacks in a network • Deploy system firewalls against attacks • Apply firewall rules	3

Textbook	• Pfleeger, C.P., Security in Computing 5th Edition. • Cryptography and Network Security by William Stalling, 2011

<table>
<tr><td rowspan="2">Department</td><td rowspan="2">Computer Engineering and Information Technologies</td><td rowspan="2">Major</td><td colspan="6" rowspan="2">Cyber Security</td></tr>
<tr></tr>
<tr><td>Course Name</td><td>Foundation of Computer Programming</td><td>Course Code</td><td colspan="6">CYBR 351</td></tr>
<tr><td rowspan="2">Prerequisites</td><td rowspan="2"></td><td rowspan="2">Credit Hours CRH</td><td colspan="2">4</td><td colspan="2">CTH</td><td colspan="2">6</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>4</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: Credit Hours L: Lecture P: Practical T: Tutorial CTH: Contact Hours</td></tr>
</table>

Course Description:

This course provides students with the required knowledge and skills to write their own applications. In this course, students will learn an introduction to algorithms and problem-solving skills. later in the course, students will master the basics of any programming language structure. variables, mathematical operations, conditional controlling components, looping components, arrays, functions and basic file system operations are all skills a student will learn in this course.

Topics:

- Basics of Computing and programming
- Discovering Input, output, and processing
- Understanding decision structures in programming languages
- Understanding repetition structure and its uses in programming languages
- Understanding functions and modules concepts
- Working with file systems
- Working on Debugging and exception
- Working with lists, sets, dictionaries, tuples.
- Object-oriented programming

Experiments:

References:

- Starting Out with Python
- How to Think Like a Computer Scientist: Learning with Python 3

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Introduction to Computers and Programming** • What is computer applications • Why have computer applications • How computer stores data • How computer programs work	2
2	**Input, Processing, and Output** • Program development cycle • Pseudocode • Flowcharts • Working with variables with different data types • Reading input from the user • Printing program output on the screen	2
3	**Decision Structures and Boolean Logic** • Logical Operators • If Statement • If-else statement • Nested conditions	1
4	**Repetition Structures** • Condition-controlled vs count-controlled repetition • While loop • For loop • Nested loop	2
5	**Functions and Modules** • Modularizing program with functions • Void functions • Local vs global variables • Passing arguments to functions • Value return functions • Working with modules	4
6	**Files and Exceptions** • Types of files • File access methods • Reading files • Writing to files • File processing operations • Exceptions	4
7	**More About Strings** • String processing operations • Testing, searching and manipulating strings	1
8	**Lists and Tuples** • Basics of sequencing • Basics of lists and tuples	3

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	• iterations in lists and tuples • Lists operations • Tuples operations	
9	**Dictionaries and Sets** • Basics of key value pairs • Basics of dictionary and sets • iterations in dictionary and sets • Dictionary operations • sets operations	3
10	**Classes and Object-Oriented Programming** • Procedural and Object-Oriented Programming • Classes • Working with Instances • Techniques for Designing Classes	4
Textbook	• Starting Out with Python • How to Think Like a Computer Scientist: Learning with Python 3	

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	Lab 1: Working with pseudocode	2
2	Lab 2: Working with flowcharts	2
3	Lab 3: setup python programming language development environment	3
4	Lab 3: Working with if statement and logical operators	3
5	Lab 4: Working with if else statement	3
6	Lab 5: working with WHILE loop	2
7	Lab 6: Working with FOR loop	2
8	Lab 7: Working with functions	4
9	Lab 8: working with modules	4
10	Lab 9: Working with files	4
11	Lab 10: handling exceptions	4
12	Lab 11: Working with strings	4
13	Lab 12: Working with lists and tuples	5
14	Lab 13: Working with dictionary and sets	5
15	Lab 14: Working with Object-oriented programming	5
Textbook	• Starting Out with Python • How to Think Like a Computer Scientist: Learning with Python 3	

<table>
<tr><td><b>Department</b></td><td><b>Computer Engineering and Information Technologies</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Operating Systems’ Security</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR312</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>INSA 312 & CYBR 321</b></td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3">4</td><td colspan="2">CTH</td><td>6</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>4</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

This course provides basic concepts of architecture and security of different Operating Systems including Windows, Linux, and Macintosh. The course of OSs security encompasses many different techniques and methods, which ensure safety from threats and attacks. OSs security module includes different applications and programs to perform required tasks and stop unauthorized interference. The course will cover security in User Registration and privileges security, File System security, User access control and Network security of the Operating Systems. A brief overview of User and Kernel Space is also included in the scope.

Topics:

- Basic concepts of Operating System Security and its domains
- Differences between well-known operating systems
- Standards in Operating System Security and their advantages
- The architecture of an Operating System’s File system
- Processes involved in Intercommunications of different programs and processes
- User Access and User Authorization mechanisms of different Operating System
- Operating System vulnerabilities and their security countermeasures
- Network Security basic concepts
- Tools associated with network security in Operating System
- Malware injection in an Operating System and its countermeasures

Experiments:

References:

- Trent Jaeger: Operating System Security
- Andrew S. Tanenbaum: Modern Operating Systems

Detailed of Theoretical Contents		
No.	Contents	Hours
1	**Chapter 2: Kernel Space and User Space** • Introduction to User Space and Kernel • Interconnection of Kernel and User Space	1
2	**Chapter 3: OS basic features and requirements** • Basic Security aspects of OS • Vulnerabilities of OS	2
3	**Chapter 4: File System in an OS** • Types of System Files • Purpose of different System Files • File System Architecture of different OS	1
4	**Chapter 5: Security and Threats to OS** • Security of a File System in OS • Vulnerabilities to File System • Countermeasures ○ Tools ○ Practices	3
5	**Chapter 6: Access Control in OS** • Access Control Mechanisms in OS • Access Control Advantages and Disadvantages	3
6	**Chapter 7: User Management** • User Registration and Authorization • User Privileges and requirements • Vulnerabilities in User Registration • Countermeasures against Vulnerabilities	3
7	**Chapter 9: Security issues in OS Processes** • Inter-process communication vulnerabilities • Inter-process communication security measures	2
8	**Chapter 10: Security issues in User Space** • User Mode Basics • User Mode Vulnerabilities • User Mode Security Countermeasures	3
9	**Chapter 11: Security issues in Kernel Space** • Kernel Mode Basics • Kernel Mode Vulnerabilities • Kernel Mode Security Countermeasures • Kernel Debugging • Kernel Auditing • Kernel Forensics	3
10	**Chapter 12: Security issues with Hardware** • Kernel and Hardware Mechanisms • Hardware Interface with OS • OS security on Hardware Interfaces	2
11	**Chapter 13: Introduction to Mobile OS** • Mobile OS fundamentals	1

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	• Multi-user interface • Multi-app interface	
12	**Chapter 14: Security issues in Mobile OS** • Mobile OS Vulnerabilities • Mobile OS Security Countermeasures	2

Textbook	• Trent Jaeger: Operating System Security • Andrew S. Tanenbaum: Modern Operating Systems

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**Lab 1: Windows Security** • Analyze Windows User Authorization Security • Apply known attacks on Authorization System	3
2	**Lab 2: Windows Security Analysis-II** • Analyze Windows File System • Apply known attacks on the windows file system	3
3	**Lab 3: Windows Security Analysis-III** • Analyze Access Control Security in Windows • Apply known attacks on windows access control	3
4	**Lab 4: Linux Security-I** • Analyze Linux User Authorization Security • Apply known attacks on Authorization System	3
5	**Lab 5: Linux Security-II** • Analyze Linux File System Security • Apply known attacks on File System	3
6	**Lab 6: Linux Security-III** • Analyze Linux Access Control Security • Apply known attacks on Access Control System	3
7	**Lab 7: Mac OS Security-I** • Analyze Mac User Authorization Security • Apply known attacks on Authorization System	5
8	**Lab 8: Mac OS Security-II** • Analyze Mac File System Security • Apply known attacks on File System	5
9	**Lab 9: Mac OS Security-III** • Analyze Mac Access Control Security • Apply known attacks on Access Control System	5
10	**Lab 10: Analyze Network Security in Windows** • OS Firewall • OS Antivirus	5
11	**Lab 11: Analyze Network Security in Linux** • OS Firewall • OS Antivirus	5
12	**Lab 12: Analyze Network Security in Mac OS** • OS Firewall • OS Antivirus	5
13	**Lab 13: Malware Injection** • Malware Injection in OS • Apply countermeasures to disinfect the system	4

Textbook	• Trent Jaeger: Operating System Security • Andrew S. Tanenbaum: Modern Operating Systems

<table>
<tr><td><b>Department</b></td><td><b>Engineering of Computer and Information Technology</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Applied Cryptography</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR322</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>MATH304, CYBR321</b></td><td rowspan="2"><b>Credit Hours</b>
<b>CRH</b></td><td colspan="3">3</td><td colspan="2">CTH</td><td>3</td></tr>
<tr><td>L</td><td>3</td><td>P</td><td>0</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description :

This course is a comprehensive introduction to modern cryptography and its related standards. The course emphasis on the application and implementation of various techniques for achieving message confidentiality, integrity, authentication, and non-repudiation. Topics include: Symmetric ciphers; Classical encryption techniques; Block ciphers (DES, AES); Block cipher operation; Random bit generation; Stream ciphers; Asymmetric ciphers (RSA, Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Cryptography); Cryptographic data integrity algorithms (Cryptographic hash functions; Message authentication codes; Digital signatures). Key management and distribution

Topics :

- Introduction to Cryptography & Network Security
- Symmetric Ciphers
- Asymmetric Ciphers
- Cryptographic Data Integrity Algorithms
- Key Management and Distribution

Experiments:

References :

Cryptography and Network Security: Principles and Practice, William Stallings, 7 Edition, 2017

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Introduction to Cryptography & Network Security** • Computer Security Concepts • The OSI Security Architecture • Security Attacks • Security Services • Security Mechanisms • Fundamental Security Design Principles • Attack Surfaces and Attack Trees • A Model for Network Security • Standards	2
2	**Symmetric Ciphers** • **Classical Encryption Techniques** o Symmetric Cipher Model o Substitution Techniques o Transposition Techniques o Rotor Machines o Steganography	2
3	**Symmetric Ciphers** • **Block Ciphers and the Data Encryption Standard** o Traditional Block Cipher Structure o The Data Encryption Standard o A DES Example o The Strength of DES o Block Cipher Design Principles	2
4	**Symmetric Ciphers** • **Advanced Encryption Standard** o AES Structure o AES Transformation Functions o AES Key Expansion o An AES Example o AES Implementation	3
5	**Symmetric Ciphers** • **Block Cipher Operation** o Multiple Encryption and Triple DES o Electronic Codebook o Cipher Block Chaining Mode o Cipher Feedback Mode o Output Feedback Mode o Counter Mode o XTS-AES Mode for Block-Oriented Storage Devices o Format-Preserving Encryption	3
6	**Symmetric Ciphers** • **Random Bit Generation and Stream Ciphers**	3

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	○ Principles of Pseudorandom Number Generation ○ Pseudorandom Number Generators ○ Pseudorandom Number Generation Using a Block Cipher ○ Stream Ciphers ○ RC4 ○ True Random Number Generators	
7	**Asymmetric Ciphers** • **Public-Key Cryptography and RSA** ○ Principles of Public-Key Cryptosystems ○ The RSA Algorithm	6
8	**Asymmetric Ciphers** • **Other Public-Key Cryptosystems** ○ Diffie-Hellman Key Exchange ○ Elgamal Cryptographic System ○ Elliptic Curve Arithmetic ○ Elliptic Curve Cryptography ○ Pseudorandom Number Generation Based on an Asymmetric Cipher	6
9	**Cryptographic Data Integrity Algorithms** • **Cryptographic Hash Functions** ○ Applications of Cryptographic Hash Functions ○ Two Simple Hash Functions ○ Requirements and Security ○ Hash Functions Based on Cipher Block Chaining ○ Secure Hash Algorithm (SHA) ○ SHA-3	3
10	**Cryptographic Data Integrity Algorithms** • **Message Authentication Codes** ○ Message Authentication Requirements ○ Message Authentication Functions ○ Requirements for Message Authentication Codes ○ Security of MACs ○ MACs Based on Hash Functions: HMAC ○ MACs Based on Block Ciphers: DAA and CMAC ○ Authenticated Encryption: CCM and GCM ○ Key Wrapping ○ Pseudorandom Number Generation Using Hash Functions and MACs	3
11	**Cryptographic Data Integrity Algorithms** • **Digital Signatures** ○ Digital Signatures ○ Elgamal Digital Signature Scheme ○ Schnorr Digital Signature Scheme ○ NIST Digital Signature Algorithm ○ Elliptic Curve Digital Signature Algorithm ○ RSA-PSS Digital Signature Algorithm	3

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
12	**Key Management and Distribution** • Symmetric Key Distribution Using Symmetric Encryption • Symmetric Key Distribution Using Asymmetric Encryption • Distribution of Public Keys • X.509 Certificates • Public-Key Infrastructure	3
Textbook	Cryptography and Network Security: Principles and Practice, William Stallings, 7 Edition, 2017	

<table>
<tr><td><b>Department</b></td><td><b>Engineering of Computer and Information Technology</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Advanced Programming</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR352</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>CYBR351</b></td><td rowspan="2"><b>Credit Hours</b>
<b>CRH</b></td><td colspan="2">4</td><td colspan="2">CTH</td><td colspan="2">6</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>4</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description :

This course extends the study of basic programming principles introduced in the Foundation of Computer Programming course (CYBR351). The course covers web-development techniques in client side that use HTML5, CSS, and JavaScript as web development essentials. In addition, students will learn database basics; SQL and Server side programming.

Topics :

- The Internet and the World Wide Web
- HyperText Markup Language (HTML) for authoring web pages
- Cascading Style Sheets (CSS) for applying stylistic information to web pages
- JavaScript for creating interactive web pages
- PHP Hypertext Processor for generating dynamic pages on a web server
- Databases fundamentals and SQL
- PHP and MySQL
- Asynchronous JavaScript and XML (Ajax) for enhanced web interaction and applications

Experiments:

References :

- Web Programming Step by Step, 2nd Edition, by Stepp/Kirst/Miller
- Web Programming and Internet Technologies, 2nd Edition by Scobey

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**The Internet and the World Wide Web:** • The Internet: o History o People and Organizations o Technologies • The World Wide Web (WWW): o Clients and Servers Architecture o URLs and DNS o Hypertext Transmit Protocol (HTTP) o Languages of the Web	**2**
2	**HyperText Markup Language (HTML):** • HTML versions • Semantic and presentational HTML • The structure and syntax of an HTML document • Links • Classic document elements • Lists • Images • Tables • Forms • HTML5-specific tags	**3**
3	**Cascading Style Sheets (CSS):** • BASIC CSS o CSS Syntax o Applying CSS to a Web Page o Color Properties o CSS Comments • CSS Properties o Font Properties o Text Properties o Background Properties o List Properties o Table Properties • More CSS Syntax o Style Inheritance and Conflicts o IDs and ID Selectors o Classes and Class Selectors o Pseudo-class Selectors o W3C CSS Validator	**3**
4	**JavaScript:** • Key JavaScript Concepts o Client-Side Scripting o Event-Driven Programming o A JavaScript Program o The Document Object Model (DOM) • JavaScript Syntax	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	○ Types ○ Numbers and Arithmetic ○ Variables ○ Comments ○ Using DOM Objects ○ Debugging Common Errors ○ Strings ○ for Loops ○ The Math Object ○ Null and Undefined Values • Program Logic ○ Comparison Operators ○ Conditional Statements: if/else ○ Boolean Values ○ Logical Operators ○ While Loops • Advanced JavaScript Syntax ○ Scope and Global Variables ○ Arrays ○ Function Parameters and Returns ○ Input Dialog Boxes	
5	**PHP:** • Server-Side Basics ○ The lifecycle of a Web Request ○ Introduction to PHP • PHP Basic Syntax ○ Syntax Errors ○ The print Statement ○ Types ○ Arithmetic ○ Variables ○ Strings ○ Comments ○ Boolean Logic ○ Control Statements ○ Errors and Debugging • Embedded PHP ○ Embedding PHP in HTML ○ Expression Blocks • Advanced PHP Syntax ○ Functions ○ Including Files ○ Arrays ○ The foreach Loop ○ File I/O ○ Classes and Objects	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
6	**Databases fundamentals and SQL :** • Relational Databases • Database Design Goals • Some Architectural Aspects of a “Good” Database • SQL o Connecting to MySQL o Database/Table Information o The SELECT Statement o Filtering Results with the WHERE Clause o Ordering Results: ORDER BY o Aggregating Data: GROUP BY, HAVING o Modifying Data: INSERT, EDIT, and DELETE	**3**
7	• **PHP and MySQL:** • phpMyAdmin o Creating databases o Creating and managing users o Creating and managing database tables • MySQLi in PHP o Connecting to the database o Writing a MySQL query in PHP o Fetching the result (data query) o Updating data	**5**
8	**Asynchronous JavaScript and XML (Ajax)** • XML o What is XML? o XML Document Structure, Schemas, and DTDs o Processing XML Data • AJAX CONCEPTS o History and Compatibility • USING XMLHTTPREQUEST TO FETCH DATA o Synchronous Requests o Checking for Ajax Errors o Asynchronous Requests o Prototype's Ajax Features • Ajax Security and Debugging	**4**
Textbook	• Web Programming Step by Step, 2nd Edition, by Stepp/Kirst/Miller • Web Programming and Internet Technologies, 2nd Edition by Scobey	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	Lab: HTTP request and response (demonstrate Web browsers and Web servers communication)	**4**
2	Lab: HTML	**6**
3	Lab: Cascading Style Sheets (CSS)	**6**
4	Lab: JavaScript	**6**
5	Lab: PHP	**8**
6	Lab: SQL	**6**
7	Lab: PHP and MySQL	**8**
1	Lab: AJAX	**8**
Textbook	• Web Programming Step by Step, 2nd Edition, by Stepp/Kirst/Miller • Web Programming and Internet Technologies, 2nd Edition by Scobey	

Textbooks	• Web Programming Step by Step, 2nd Edition, by Stepp/Kirst/Miller
	• Web Programming and Internet Technologies, 2nd Edition by Scobey

<table>
<tr><td><b>Department</b></td><td><b>Engineering of Computer and Information Technology</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Secure Software Development</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR453</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>CYBR352</b></td><td rowspan="2"><b>Credit Hours</b>
<b>CRH</b></td><td colspan="2">4</td><td colspan="2">CTH</td><td colspan="2">6</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>4</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description :

This course focuses on integrating security in the Software Development Life Cycle (SDLC). It covers the best practices that the software developer needs to avoid opening up their users, customers, and organization to attack at the application layer. In this course, students will learn how to identify and apply security controls in development environments; Assess the effectiveness of software security; Define and apply secure coding guidelines and standards.

Topics :

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance, and Disposal

Experiments:

References :

- Official (ISC)2 Guide to the CSSLP CBK ((ISC)2 Press) 2nd Edition by Mano Paul
- Core Software Security by James Ransome and Anmol Misra
- OWASP WebGoat Project, https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Secure Software Concepts:** ○ Holistic Security ○ Core Security Concepts ○ Design Security Concepts ○ Risk Management ○ Security Policies: The ‘What’ and ‘Why’ for Security ○ Software Development Methodologies ○ Regulations, Privacy and Compliance	**3**
2	**Secure Software Requirements:** ○ Sources for Security Requirements ○ Policy Decomposition ○ Data Classification ○ Subject/Object Matrix ○ Requirements Traceability Matrix (RTM)	**5**
3	**Secure Software Design:** ○ The Need for Secure Design ○ Design Processes ○ Architectures ○ Technologies	**3**
4	**Secure Software Implementation/Coding:** ○ Who is to be Blamed for Insecure Software? ○ Common Software Vulnerabilities and Controls ○ Defensive Coding Practices – Concepts and Techniques ○ Secure Software Processes	**5**
5	**Secure Software Testing:** ○ Quality Assurance ○ Attack Surface Validation (Security Testing) ○ Test Data Management	**3**
6	**Software Acceptance:** ○ Guidelines for Software Acceptance ○ Verification and Validation (V&V)	**3**
7	**Software Deployment, Operations, Maintenance, and Disposal:** ○ Installation and Deployment ○ Operations and Maintenance ○ Disposal	**4**
Textbook	• Official (ISC)2 Guide to the CSSLP CBK ((ISC)2 Press) 2nd Edition by Mano Paul • Core Software Security by James Ransome and Anmol Misra	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	Lab1: Install Lab Environment: 1. Hypervisor: VMWare Workstation Player 12 for Windows OR VMWare Workstation Player 12 for Linux 2. OWASP WebGoat VM: This virtual machine houses the Web Application (WebGoat) which will be tested. 3. Kali Linux (64-bit VM): This virtual machine houses the tools (ZAProxy, NMAP, etc.) to be used to test the Web Application (WebGoat)	**6**
2	Lab2: HTTP basics & proxy	**3**
3	Lab3: Injection Flaws (SQL Injection)	**3**
4	Lab4: Authentication Flaws (Authentication Bypasses)	**3**
5	Lab5: Authentication Flaws (JWT)	**3**
6	Lab6: Authentication Flaws (Password Reset)	**3**
7	Lab7: Cross-Site Scripting (XSS)	**3**
8	Lab8: Access Control Flaws (Direct Object References)	**3**
9	Lab9: Access Control Flaws (Missing Function Level Access Control)	**3**
10	Lab10: Insecure Communication (Insecure Login)	**3**
11	Lab11: Cross-site request forgery (XSS)	**3**
12	Lab12: Vulunerable Components	**4**
13	Lab13: Client Side (Bypass Front-End restrictions)	**4**
14	Lab14: Client Side (Client Side Filtering)	**4**
15	Lab15: Client Side (HTML Tampering)	**4**
Textbook	• OWASP WebGoat Project, https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project	

Detailed of Practical Contents

Chapter.	Contents	Hours
	• Official (ISC)2 Guide to the CSSLP CBK ((ISC)2 Press) 2nd Edition by Mano Paul • Core Software Security by James Ransome and Anmol Misra	

<table>
<tr><td><b>Department</b></td><td><b>Engineering of Computer and Information Technology</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Networks & Communications Security</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR 441</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>INET313 and CYBR322</b></td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2"><b>4</b></td><td colspan="2"><b>CTH</b></td><td colspan="2">6</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>4</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

The course covers the theory and practice of network and communication security, focusing in particular on the security aspects of the network. The different weakness in routers, switches, and transmission channel will be represented. The different security protocols will be studied, discussed and implemented AAA, IPS/IDS, VPN, MPLS, SET, and PKI over routers or firewalls.

Topics :

Upon successful completion of this course, students will be able to:

- Identify the fundamental concepts of network and communication security.
- Identify security threats and vulnerabilities.
- Identify and implement access control and account management security measures.
- IDS/IPS
- Configure Firewalls and UTM
- Configure SET
- Kerberos
- Switch security
- Configure VPN layer 2 and 3 with different protocols

Experiments:

- Routers
- Switches
- Firewall

References :

- ✓ CCNA Security, Cisco Networking Academy,
- ✓ Security of Information and Communication Networks, by Stamatios V. Kartalopoulos, 2009
- ✓ Network Security: Data and Voice Communications (McGraw-Hill Series on Computer Communications), 1995

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Security Fundamentals in communication system:** • Concepts • Threats • Attacks • Vulnerabilities	**2**
2	**User Authentication:** • Describe AAA, Kerberos • Describe TACACS+ and Radius protocols.	**2**
3	**IDS/IPS** • Explain the functions and operations of IDS and IPS systems. • Describe the characteristics of IPS signatures. • Explain how signature alarms are used in Cisco IPS solutions. • Describe the purpose of tuning signature alarms in a Cisco IPS solution. • Explain how the signature actions in a Cisco IPS solution affect network traffic.	**3**
4	**Layer 2 Security:** • Attack types • Mitigating layer attacks • Layer 2 best practice	**3**
5	**Implementing Virtual Private Networks:** • Describe VPNs and their benefits • VPN layer 2 and 3 • VPN Architecture • PPTP protocol • L2TP protocol • IPsec protocol • GRE Protocol • MPLS Protocol	**3**
6	**Firewalls:** • Concepts • Describe the purpose and operation of firewall technologies • Zone-based Policy Firewall and DMZ zone	**3**
7	**Unified threats Management:** • What is Unified Threat Management • Unified Threat Management (UTM) Appliance Comparison • Fortinet Technologies • Sophos Technologies • Palo Alto Technologies	**3**
8	**Secure Electronic Transaction** • Describe SET protocol • SET Architecture	**3**
9	**Multimedia communication Security** • Multimedia concepts • Attacks • Multimedia security techniques	**4**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
Textbook	✓ CCNA Security, Cisco Networking Academy, ✓ Security of Information and Communication Networks, by Stamatios V. Kartalopoulos, 2009 ✓ Network Security: Data and Voice Communications (McGraw-Hill Series on Computer Communications), 1995	

Detailed of Practical Contents		
Chapter.	Contents	Hours
1	**Lab: Securing the Router for Administrative Access:** • Control Administrative Access for Routers • Configure Administrative Roles • Configure Cisco IOS Resilience and Management Reporting	2
2	**Lab: User Authentication: Securing Administrative Access Using AAA and RADIUS** • Configure the local user database using Cisco IOS. • Configure AAA local authentication using Cisco IOS. • Configure users on the RADIUS server. • Use the Cisco IOS to configure AAA services on a router to access the RADIUS server for authentication.	2
3	**Lab: IPS/IDS:** • Configure IOS Intrusion Prevention System (IPS) • Modify IPS Signatures. • Log IPS messages to a syslog server. • Use a scanning tool to simulate an attack.	5
4	**Lab: Layer 2 security:** • Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks • Describe best practices for implementation • Describe how PVLANs can be used to segregate network traffic at Layer 2	5
5	**Lab: Configuring a Site-to-Site VPN Using Cisco IOS:** • Configure VPN Layer 2 • Configure MPLS VPN Layer2. • Configure IPsec VPN settings on two routers • Configure VPN witch GRE • Configure MPLS VPN layer 3 • Configure BGP MPLS VPN • Interconnecting between VPN layer 2 and VPN Layer 3	7
6	**Lab: Firewalls: Implementing Cisco the Adaptive Security Appliance** • Describe and compare Concepts ASA solutions to other routing firewall technologies. • Describe the default configuration of an ASA 5505 • Configure an ASA to provide basic firewall services. • Configuring Basic ASA Settings and Interface Security Levels • Explain and configure objects groups on an ASA. • Explain and configure access lists with objects groups on an ASA. • Configure an ASA to provide NAT, DMZ, DHCP, ACL services • Configure access control using the local database and AAA server..	7
7	**Lab: FortiGate UTM configuration** • FortiGate Installation & Setup	7

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
	• Security Policies & Firewall Objects • High-Availability & Traffic Shaping • Wireless Security • SSL And IPsec VPN • IPS	
8	**Lab: Installing and Configuring Palo Alto:** • Install Licenses • Configure Dynamic Updates • Configure Interfaces, VLANs, appropriate switch tagging • Setup DHCP Server(s) • Configure Zones • Configure Network Address Objects • Create Security Policies • Create NAT Policies • Ingress and Egress	**7**
9	**Lab: Administering Sophos SG UTM**: • Configure a UTM using the Setup Wizard • Navigate the WebAdmin • Configure system settings • Configure interfaces and routing • Create firewall rules • Demonstrate Advanced Threat Protection • Configure Intrusion Prevention (IPS) • Configure an SSL site-to-site VPN • Configure an IPsec site-to-site VPN • Deploy the HTTPS CA certificate • Configure Filter Actions SG UTM Sophos Certified Administrator • Configure Web Policies • Configure Web Profiles • Configure Application Control	**7**
10	**Lab: Voice over IP Security:** • Simulated VoIP attacks • Configure a countermeasure	**3**
Textbook	✓ CCNA Security, Cisco Networking Academy, ✓ Security of Information and Communication Networks, by Stamatios V. Kartalopoulos, 2009 ✓ Network Security: Data and Voice Communications (McGraw-Hill Series on Computer Communications), 1995	

<table>
<tr><td><b>Department</b></td><td><b>Engineering of Computer and Information Technology</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Advanced Technologies in Networks Security</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR442</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>CYBR441</b></td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2"><b>4</b></td><td colspan="2"><b>CTH</b></td><td colspan="2">6</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>4</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description :

This course provides an in-depth review of the theoretical and applied topics in network security. Students satisfactorily completing the course will be able to formulate a security model for network environments, and apply cryptography, protocol design, and emergent network security technologies to meet the requirements of that model. the course considers research and solutions in a broad selection of important network. In studying these environments, we consider important works in protocol design and formal analysis, advanced authentication, network configuration and management, firewalls systems, intrusion detection, and other topics.

Topics :

- Cisco ASA firewalls, Cisco ASA NGFW,
- Securing network using Cisco Routers and Cisco catalyst switches,
- Create DMVPN, FlexVPN,
- Implement Central Web Authentication (CWA),
- Describe trust solution,
- Design a highly secure wireless solution
- Implement Cisco Cloud Web Security (CWS)
- Implement Cisco Web Security Appliance (WSA)
- Implement Cisco Email Security Appliance
- Implement Cisco Next-Generation Firewall (NGFW) Security
- Implement Cisco Advanced Malware Protection (AMP)
- Implement architectures (public cloud, private cloud)
- Design a web security solution
- Implement Cisco FirePOWER Next-Generation IPS (NGIPS)

Experiments:

- Routers
- Switches
- Firewall NG

References :

CCNP Security:

- Implementing Cisco Secure Access Solutions (SISAS)
- Implementing Cisco Edge Network Security Solutions (SENSS)
- Implementing Cisco Secure Mobility Solutions (SIMOS)
- Implementing Cisco Threat Control Solutions (SITCS)

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Threat Defense** • Describe SGA ACLs • Describe Cisco TrustSec and MACsec Features • SGT Classification – dynamic/static • Describe threat detection features • Implement botnet traffic filtering • Configure application filtering and protocol inspection • Describe ASA security contexts • Threat Defense Architectures	**3**
2	**Network Threat Defense** • Cisco Next-Generation Firewall (NGFW) Security Services • Implement application awareness • Implement access control policies (URL-filtering, reputation-based, file filtering) • Configure and verify traffic redirection • Implement Cisco AMP for Networks	**3**
3	**Cisco Advanced Malware Protection (AMP)** • Describe cloud detection technologies • Compare and contrast AMP architectures (public cloud, private cloud) • Configure AMP endpoint deployments • Describe analysis tools • Describe incident response functionality • Describe sandbox analysis • Describe AMP integration	**2**
4	**Implement Central Web Authentication (CWA)** • Describe the function of CoA to support web authentication • Configure the authentication policy to facilitate CWA • URL redirect policy • Redirect ACL • Customize web portal • Verify central web authentication operation	**2**
5	**Secure Communications** • Site-to-site VPNs on routers and firewalls • Describe GETVPN • Implement IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6) • Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6) • Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA • Implement remote access VPNs • Implement AnyConnect IKEv2 VPNs on ASA and routers • Implement AnyConnect SSL VPN on ASA and routers • Implement clientless SSL VPN on ASA and routers	**3**
6	**Cisco Web Security Appliance (WSA)** • Describe the features and functionality • Implement data security	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	• Implement WSA identity and authentication, including transparent user identification • Implement web usage control • Implement AVC • Implement antimalware and AMP • Implement decryption policies • Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)	
7	**Cloud Web Security** • Cisco Cloud Web Security (CWS) • Describe the features and functionality • Implement the IOS and ASA connectors • Implement the Cisco AnyConnect web security module • Implement web usage control • Implement AVC • Implement antimalware • Implement decryption policies	**2**
8	**Cisco FirePOWER Next-Generation IPS (NGIPS)** • Configurations • Describe traffic redirection and capture methods • Describe preprocessors and detection engines • Implement event actions and suppression thresholds • Implement correlation policies • Describe SNORT rules • Implement SSL decryption policies	**3**
9	**Deployments NGIPS** • Deploy inline or passive modes • Deploy NGIPS as an appliance, virtual appliance, or module within an ASA • Describe the need for traffic symmetry • Compare inline modes: inline interface pair and inline tap mode	**2**
10	**Security Architectures** • Design a web security solution • Compare and contrast Cisco FirePOWER NGFW, WSA, and CWS Compare and contrast physical WSA and virtual WSA • Describe the available CWS connectors	**2**
11	**Design an email security solution** • Compare and contrast physical ESA and virtual ESA • Describe hybrid mode Design Cisco FirePOWER solutions • Configure the virtual routed, switched, and hybrid interfaces • Configure the physical routed interfaces	**1**
Textbook	• Implementing Cisco Secure Access Solutions (SISAS) • Implementing Cisco Edge Network Security Solutions (SENSS) • Implementing Cisco Secure Mobility Solutions (SIMOS) • Implementing Cisco Threat Control Solutions (SITCS)	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab: Threat Defense** • Implement FW • Implement Cisco TrustSec and MACsec Features • Implement botnet traffic filtering • Configure application filtering and protocol inspection	**2**
2	**Lab: Network Threat Defense** • Implement application awareness in NGFW • Implement access control policies (URL-filtering, reputation-based, file filtering) • Implement Cisco AMP for Networks	**2**
3	**Lab: Cisco Advanced Malware Protection (AMP)** • Configure AMP endpoint deployments • Implement antimalware and AMP • AMP Analysis Tools	**4**
4	**Lab: Implement Central Web Authentication (CWA)** • Configure the authentication policy to facilitate CWA • URL redirect policy • Redirect ACL • Customize web portal	**4**
5	**Lab: Secure Communications** • Implement IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6) • Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6) • Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA • Implement remote access VPNs • Implement AnyConnect IKEv2 VPNs on ASA and routers • Implement AnyConnect SSL VPN on ASA and routers • Implement clientless SSL VPN on ASA and routers	**6**
6	**Lab: Cisco Web Security Appliance (WSA)** • Implement data security • Implement WSA identity and authentication, including transparent user identification • Implement web usage control • Implement AVC • Implement antimalware and AMP • Implement decryption policies • Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)	**6**
7	**Lab: Cloud Web Security** • Implement the IOS and ASA connectors • Implement the Cisco AnyConnect web security module • Implement web usage control • Implement AVC	**6**

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
	• Implement antimalware • Implement decryption policies	
8	**Lab: Cisco FirePOWER Next-Generation IPS (NGIPS)** • Configurations • Implement event actions and suppression thresholds • Implement correlation policies • Implement SSL decryption policies	**8**
9	**Lab: Deployments NGIPS** • Deploy inline or passive modes • Deploy NGIPS as an appliance, virtual appliance, or module within an ASA • Compare inline modes: inline interface pair and inline tap mode	**5**
10	**Lab: Security Architectures** • Design a web security solution • Configure Cisco FirePOWER NGFW, WSA, and CWS • Compare and contrast physical WSA and virtual WSA	**5**
11	**Lab: Design an email security solution** • Configure the virtual routed, switched, and hybrid interfaces • Configure the physical routed interfaces	**4**

Textbook	• Implementing Cisco Secure Access Solutions (SISAS) • Implementing Cisco Edge Network Security Solutions (SENSS) • Implementing Cisco Secure Mobility Solutions (SIMOS) • Implementing Cisco Threat Control Solutions (SITCS)

Department	**Computer Engineering and Information Technologies**	**Major**	**Cyber Security**					
Course Name	**Wireless Network Security**	**Course Code**	**CYBR443**					
Prerequisites	**CYBR 441**	**Credit Hours CRH**	3			CTH		4
			L	2	P	2	T	0

CRH: **Credit Hours** L: **Lecture** P: **Practical** T: **Tutorial** CTH: **Contact Hours**

Course Description:

In a mobile world, the ability to gain network access in a convenient manner, but yet securely, is becoming more and more of a requirement. This course covers the basics of networking, wired networks, wireless networks, the architecture of wireless networks, security challenges in wireless networks and technology used for security of wireless networks. This course also will explore the wireless standards, authentication issues, common configuration models for commercial versus institution installs and analyze the security concerns associated with ad-hoc and standards-based methods of networking. The course also gives insight into the basics of large scale networks, their applications and security standards. From this course, the student will gain an understanding of wireless networking, protocols, and standards and security issues.

Topics:

- Basic concepts of Wireless Networking
- Difference between Wireless and Wired Networks
- Pros and Cons of Wireless Networks
- The architecture of Wireless Networks
- Design and Planning of Wireless Networks
- Security challenges to a wireless network
- Tools and Techniques to enhance security
- Mobile architecture
- Operating systems in Mobile
- Mobile hacking and security

Experiments:

References:

- LTE Security, John Wiley & Sons, 2010. Edney, Arbaugh
- Real 802.11 Security, Addison-Wesley 2004
- Wireless and Mobile Network Security, Chaouchi, Hakima, 2009. Pub: John Wiley & Sons Inc
- Advanced penetration testing, Wil Allsopp, Publisher Wiley 2016

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Chapter 1: RF Signals, Modulation, and Antennas** • RF signals • Modulations • Antennas	1

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
2	**Chapter 2: Wireless Networks Basics** • Technology • Infrastructure • Types • Standards and Protocols	1
3	**Chapter 3: Designing Wireless Networks** • Principles Governing in Designing of Wireless Networks • Deployment Procedures	2
4	**Chapter 4: Wireless network security** • Types of wireless Encryption • Wireless network threats	2
5	**Chapter 5: Wireless Vulnerabilities** • Reconnaissance Attacks • DoS Attacks • Authentication Attacks • WEP Keystream and Plaintext Recovery • WEP Key Recovery Attacks • Attacks on EAP Protocols • Rogue APs	2
6	**Chapter 6: Wireless Hacking** • Methodology • Tools • Bluetooth hacking	3
7	**Chapter 7: Wireless security tools** • Countermeasures • Tools (WIPS, AirManaget, AirDefensem Aruba RFProtect)	2
8	**Chapter 8: Mobile Network Architecture** • GSM, • GPRS • UMTS • LTE • 5G	3
9	**Chapter 9: Mobile Operating system** • Android OS Architecture • iOS • windows phone • Blackberry	2

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
10	**Chapter 10: Mobile Attacks and Vulnerabilities** • App Stores • Mobile Malware • App Sandboxing • Device and App Encryption • OS and App Updates • Jailbreaking and Rooting • Mobile Application Vulnerabilities • Privacy Issues (Geolocation) • Excessive Permissions • Physical Attacks	3
11	**Chapter 11: Mobile hacking** • Hacking Android • Hacking iOS • Hacking windows phone • Hacking Blackberry	2
12	**Chapter 12: Mobile Pen-testing** • Android Pen-testing • iOS Pen-testing • Windows phone Pen-testing • Blackberry Pen-testing	2
13	**Chapter 13: Mobile security tools** • General guidelines for mobile security • Tools (BullGuard Mobile Security, Lookout, WISeID, Webroot, NetQin)	1
Textbook	• LTE Security, John Wiley & Sons, 2010. Edney, Arbaugh • Real 802.11 Security, Addison-Wesley 2004 • Wireless and Mobile Network Security, Chaouchi, Hakima, 2009. Pub: John Wiley & Sons Inc • Advanced penetration testing, Wil Allsopp, Publisher Wiley 2016	

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**Lab1: Overview of RF Signals** • Frequency and bandwidth • Digital modulations • Antennas	2
2	**Lab 2: Wireless Network configuration** • Basic Wireless LAN Connection Configuration • WPA and Wi-Fi Protected Access 2 (WPA 2) Configuration	2
3	**Lab 3: Access point configuration** • VLANs on Aironet Access Points Configuration • Access Point as a Workgroup Bridge, Repeater and an Extended Configuration • Lightweight AP (LAP) Registration to a Wireless LAN Controller • Unified Wireless Network Local EAP Server Configuration	2

4	**Lab 4: Wireless Reconnaissance** • Airgraph--ng • CAPR • CPG • Kismet • GISKismet	2
5	**Lab 5: Rogue Access Points** • Airbase--ng • Karmetasploit	2
6	**Lab 6: Wireless Hacking** • Aircrack ng • Cracking WEP via client • Cracking clientless WEP networks • Cracking WPA/WPA2 PSK with (Aircrack, JTR, coWPAtty, Pyrit)	3
7	**Lab 7: Wireless Authentication** • Authentication on Wireless LAN Controllers Configuration • EAP-FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration • PEAP under Unified Wireless Networks with Microsoft Internet Authentication Service (IAS)	2
8	**Lab 8: Wireless security tools** • WIPS • Wi-Fi Security Auditing Tools (AirManaget, AirDefensem Aruba RFProtect)	3
9	**Lab 9: Hacking mobile OS** • Hacking iOS • Hacking Android • Hacking BlackBerry • Hacking windows phone.	4
10	**Lab 10: Mobile Pen-testing** • Android Pen-testing • iOS Pen-testing • Windows phone Pen-testing • Blackberry Pen-testing	4
11	**Lab 11: Mobile security tools** • BullGuard Mobile Security, • Lookout, • WISeID, • Webroot, • NetQin	3
12	**Lab 12: Mobile Networks Security** • Security Analysis of Mobile Networks • Tools being used to secure mobile Network	3
Textbook	• LTE Security, John Wiley & Sons, 2010. Edney, Arbaugh • Real 802.11 Security, Addison-Wesley 2004	

	• Wireless and Mobile Network Security, Chaouchi, Hakima, 2009. Pub: John Wiley & Sons Inc • Advanced penetration testing, Wil Allsopp, Publisher Wiley 2016

<table>
<tr><td><b>Department</b></td><td><b>Computer Engineering and Information Technologies</b></td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Cloud Computing and Virtualizations</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR444</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2"><b>CYBR 312 & INSA 444</b></td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2">4</td><td colspan="2">CTH</td><td colspan="2">6</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>4</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

This is an introductory course to understand the concepts of Cloud Computing, Virtualization and Computer Networks in general. From this course; students will gain an excellent understanding of basic concepts of Cloud Computing, Virtualization, and Computer Networks. This includes the definitions of CCV, cloud types and cloud service deployment models (IaaS, PaaS, SaaS), learn how to create virtual machines (VM) using Hypervisors (type-2), and understand Computer Networks and IP Addressing. A brief overview of the security of a Cloud System and its forensics are also included in the contents of the course.

Topics:

- Understanding Basic Concepts of Cloud Computing
- Understanding Cloud Computing Threats
- Understanding Cloud Computing Attacks
- Understanding Cloud Computing Security
- Understanding Cloud Security Tools
- Understanding Cloud Penetration Testing
- Understanding Cloud Security Standards and Features
- Understanding Cloud Auditing and Performance Monitoring
- Understanding Cloud Forensics concept and parameters

Experiments:

References:

- Barrie Sosinsky. 2011. Cloud Computing Bible (1st ed.). Wiley Publishing.
- Research papers and related publications

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Chapter 1: Introduction to Cloud Computing** • Cloud Computing Overview o Definition and Characteristics • Cloud Drivers and Adaptation Trends • Typical Cloud Enterprise Setup o Enterprise Workloads • Cloud Service Models o Public o Private o Hybrid • Cloud Deployment Models o Infrastructure as a Service (IaaS) o Process as a Service (PaaS) o Software as a Service (SaaS) o Business Process as a Service (BPaaS)	3

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	• Cloud Computing Benefits ○ Economic benefits ○ Operational benefits ○ Staffing Benefits ○ Security Benefits	
2	**Chapter 2: Virtualization in Cloud Computing** • Understanding Virtualization ○ Definition ○ How virtual machine works compared to the physical machine • Benefits of Virtualization in Cloud Computing	2
3	**Chapter 3: Cloud Threats** • An Overview of Cloud Threats • Cloud Threat Classifications ○ Data Breach/Loss ○ Abuse of Cloud Services ○ Insecure interfaces and APIs • Cloud Threat in Business ○ Insufficient Due Diligence ○ Shared Technology Issues ○ Unknown Risk Profile • Cloud Threats in Infrastructure ○ Inadequate infrastructure ○ The conflict between Client Hardening Procedure and Cloud Environment ○ Loss of Operational and Security Logs ○ Malicious Insiders • Other Cloud Threats ○ Illegal access to Cloud ○ Loss of Business Reputation due to Co-tenant Activities ○ Privilege Escalation ○ Natural Disasters ○ Hardware Failure • Cloud Threat in Traffic ○ Supply Chain Failure ○ Modifying Network Traffic ○ Isolation Failure • Cloud Provider Threats ○ Cloud Provider Acquisition ○ Management Interface Compromise ○ Network Management Failure ○ Authentication Attacks • Cloud Threats in Virtualization ○ VM-Level ○ Lack-in ○ Licensing Risks	6

	Detailed of Theoretical Contents	
No.	Contents	Hours
	o Loss of Governance o Loss of Encryption Keys • Cloud Threats in Law o Risks from Changes of Jurisdiction o Undertaking Malicious Probes or Scans o Theft of Computer Equipment o Cloud Service Termination or Failure o Subpoena and E-discovery • Cloud Threats in Data o Improper Data Handling and Disposal o Loss/Modification of Backup Data o Compliance Risks • Economic Denial of Sustainability (EDOS)	
6	**Chapter 4: Cloud Computing Attacks** • An Overview of Cloud Threats • Service Hijacking Using Social Engineering Attacks • Session Hijacking Using XSS Attack • Session Hijacking Using Session Riding • Domain Name System (DNS) Attacks • Side Channel Attacks or Cross-Guest VM Breaches • Side Channel Attack Countermeasures • SQL Injection Attacks • Cryptanalysis Attacks • Cryptanalysis Attacks Countermeasures • Wrapping Attacks • DoS and DDoS attacks	3
8	**Chapter 5: Cloud Security** • Introduction to Cloud Security • Cloud Security Control Layers • Importance of Cloud Security • Cloud Security Considerations • Placement of Security Controls in Cloud • Cloud Security Approaches o Encryption o Tokenization • Best Practices of Cloud Security • NIST Recommendations for Cloud Security • Organization / Provider Cloud Security Compliance Checklist	3
10	**Chapter 6: Cloud Security Tools** • Core CloudInspect • CloudPassage Halo • Other Tools	2
11	**Chapter 7: Cloud Penetration Testing** • An Overview of Cloud Penetration Testing	3

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	○ Definition • Key Considerations for Pen-Testing in The Cloud • Scope of Cloud Pen-Testing • Cloud Penetration Testing • Recommendation for Cloud Testing	
12	**Chapter 8: Service Level Agreements** • Cloud Service Level Agreements (SLAs) ○ Basic SLA concept ○ Parameters of SLAs ○ Transitions in SLAs	2
13	**Chapter 9: Auditing in Cloud** • Cloud Monitoring and Management • Performance Monitoring • Resource Monitoring and Management	2
Textbook	• Barrie Sosinsky. 2011. Cloud Computing Bible (1st ed.). Wiley Publishing. • Research papers and related publications	

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**Lab1: Cloud Computing Environment** • Overview of Cloud Computing Environment • The architecture of Cloud Computing • Types of Cloud Computing	2
2	**Lab 2: Virtualization in Cloud** • Virtualization Basics • Benefits of Virtualization in Clouds • Create and Run Virtual Machine using KVM VMware	4
3	**Lab 3: Implementation of IaaS** • Installing OpenStack • Implement OpenStack as IaaS • Use OpenStack as IaaS • Analyze features of IaaS	6
4	**Lab 5: Implementation of SaaS** • Understanding of a Cloud service as SaaS • Installation of a Cloud service as SaaS • Testing of SaaS ○ Performance ○ User Interface • Analyze Security of SaaS	6
5	**Lab 7: Identity Management in Cloud** • Concept of Identity Management	4

Detailed of Practical Contents		
No.	**Contents**	**Hours**
	• Implementation of Identity Management in OpenStack • Analyze features of Identity Management in OpenStack	
6	**Lab 8: Web Programming** • Concept of form and Control Validation • Development of a test program	4
7	**Lab 9: Single Sign On (SSO)** • Basic concepts of Single Sign On • Access Control and Single Sign On • Implementation of Single Sign On	4
8	**Lab 10: Cloud Security** • Install and use security features for Access Control • Implement security features for Data Directory • Encryption in Clouds • Implementation of Encryption modules on Cloud	8
9	**Lab 12: User Management in Cloud** • Create Users • User Grouping • Admin Privileges	6
10	**Lab 12: Federated Identities in Cloud** • Implement federated identities concept over 2 applications in Cloud with the same Identity	3
11	**Lab 14: Implementation of User Management Security** • Installing Administrative rules in Cloud • Testing and Improvements in Administrative measures	5

Textbook	• Barrie Sosinsky. 2011. Cloud Computing Bible (1st ed.). Wiley Publishing.

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6"><b>Cyber Security</b></td></tr>
<tr><td><b>Course Name</b></td><td><b>Penetration Testing</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR 423</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR 453</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3">4</td><td colspan="2"><b>CTH</b></td><td>6</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>4</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH<b>: Credit Hours</b> L<b>: Lecture</b> P<b>: Practical</b> T<b>: Tutorial</b> CTH<b>: Contact Hours</b></td></tr>
</table>

Course Description:

This course was designed to provide students with the tools and techniques used by hackers and information security professionals. This course will immerse students into the Hacker Mindset so that they will be able to defend against future attacks.

Students will be thought the Five phases of Ethical Hacking and thought how the student can approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks. The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach to help you identify when an attack has been used against your own targets.

Topics :

- Understand the different phase of hacking:
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Denial-of-Service
- Session Hijacking
- Social Engineering
- …

Experiments:

- Linux and Windows server
- VMware
- Software tools for different techniques.

References:

- CEHv9-10 theoretical and practice/ECCouncil

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Introduction to Ethical Hacking**: • Key issues plaguing the information security world, • Incident management process, • Phases for penetration testing	**2**
2	**Footprinting and Reconnaissance:** • Various types of footprinting • Footprinting tools • Countermeasures	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
3	**Scanning Networks:** • Network scanning techniques • Scanning countermeasures	3
4	**Enumeration:** • Enumeration techniques • Enumeration countermeasures	3
5	**System Hacking:** • System hacking methodology • Steganography • Steganalysis attacks • Covering tracks	3
6	**Malware Threats:** • Working of viruses, Trojan, worms, … • Virus, trojan analysis, • Computer worms, Bots • Malware analysis procedure • Countermeasures	3
7	**Sniffing:** • Packet sniffing techniques • Defend against sniffing	3
8	**Social Engineering:** • Social Engineering techniques • Identify theft • Social engineering countermeasures	3
9	**Denial-of-Service:** • DoS/DDoS attack techniques • Botnets, DDoS attack tools • DoS/DDoS countermeasures	2
10	**Session Hijacking:** • Session hijacking techniques • Countermeasures	3
11	**Evading IDS, Firewalls, and Honeypots:** • Firewall • IDS and honeypot evasion techniques • Evasion tools and countermeasures.	2
12	**Buffer overflow** • Buffer Overflow concepts • Buffer Overflow methodology • Buffer Overflow detection • Buffer Overflow countermeasures • Buffer Overflow security tools • Buffer Overflow pen testing	2
Textbook	**CEHv9-10 theoretical and practice/Eccouncil**	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab 1: Building your hacking lab** • VMware/Hyper V/ Xbox • Kali Linux/Parrot/NodeZero/Metasploit • Windows server/clients	**5**
2	**Lab 2: Footprinting and Reconnaissance :** (*The instructor can choose a lab according to the tools available and time*) • People Search Using Anywho and Spokeo Online Tool • Analyzing Domain and IP Address Queries Using SmartWhois • Network Route Trace Using Path Analyzer Pro • Tracing Emails Using eMailTrackerPro Tool • Collecting Information About a target's Website Using Firebug, Maltego, Foca, GHDB • Identifying Vulnerabilities and Information Disclosures Search Engines using Search Diggity	**3**
3	**Lab 3: Scanning Networks :** (*The instructor can choose a lab according to the tools available and time*) • Scanning System and Network Resources Using Advanced IP Scanner • Fingerprint Open Ports for Running Applications Using the Amap Tool • Monitor TC P/IP Connections Using die CurrPorts Tool • Scan a Network for Vulnerabilities Using GFI LanGuard • Explore and Audit a Network Using Nmap • Scanning a Network Using the NetScan Tools Pro • Drawing Network Diagrams Using LAN Surveyor • Mapping a Network Using the Friendly Pinger • Anonymous Browsing Using Proxy Switcher • Daisy Chaining Using Proxy Workbench • HTTP Tunneling Using HTTPort • Detect, Delete and Block Google Cookies Using G-Zapper • Scanning the Network Using the Colasoft Packet Builder	**7**
4	**Lab 4: Enumeration :** (*The instructor can choose a lab according to the tools available and time*) • Enumerating NetBIOS Using the SuperScan Tool • Enumerating NetBIOS Using the NetBIOS Enumerator Tool • Enumerating a LDAP with LDAP enumeration tools • Enumerating SNMP with softPerfect tools • Enumerating the System Using Hyena	**3**
5	**Lab 5: System Hacking** : (*The instructor can choose a lab according to the tools available and time*) • Extracting Administrator Passwords Using LCP • Hiding Files Using NTFS Streams • Find Hidden Files Using ADS Spy • Hiding Files Using the Stealth Files Tool • Extracting SAM Hashes Using PWdump7 Tool	**5**

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
	• Creating the Rainbow Tables Using Winrtge • Password Cracking Using RainbowCrack • Extracting Administrator Passwords Using LOphtCrack • Password Cracking Using Ophcrack • System Monitoring Using RemoteExec • Hiding Data Using Snow Steganography • Password Recovery Using CHNTPW.ISO • User System Monitoring and Surveillance Needs Using Spytech Spy Agent • Web Activity Monitoring and Recording using Power Spy • Image Steganography Using QuickStego	
6	**Lab 6: Malware Threats** (*The instructor can choose a lab according to the tools available and time*) • Creating an HTTP Trojan and remote controlling Target machine using HTTP RAT • Creating a Trojan server using GUI trojan MeSueker • Creating Botnet infrastructure using Umbra Leader • Creating a virus using the J|PS Vims Maker tool • Creating Worms using • Virus analysis using IDA Pro • Virus Analysis using Vims Total • Virus Analysis Usuig OllyDbg • Creating a Worm Using the Internet Worm Maker Thing/ Ghost eye Worm • Detecting Trojans	**5**
7	**Lab 7: Sniffing** : (*The instructor can choose a lab according to the tools available and time*) • Sniffing die network using die Colasoft Packet Builder • Sniffing die network using die OmniPeek Network Analyzer • Spooling MAC address using SMAC • Sniffing the network using die WinArpAttacker tool • Analyzing the network using the Colasoft Network Analyzer • Sniffing passwords using Wireshark • Performing a man-in-the-middle attack using Cain & Abel • Advanced ARP spoofing detection using XArp • Detecting Systems running in promiscuous mode in a network using PromqryUI • Sniffing a password from captured packets using Sniff - O - Matic	**5**
8	**Lab 8: Social Engineering:** (*The instructor can choose a lab according to the tools available and time*) • Detect phishing sites/ Netcraft/PhishTank • Protect networks from phishing attacks • Perform credential Harvesting	**3**
9	**Lab 9: Denial-of-Service :** (*The instructor can choose a lab according to the tools available and time*) • SYN flooding a target host using hping3/Metasploit	**3**

Detailed of Practical Contents		Hours
Chapter.	**Contents**	**Hours**
	- H TTP flooding using DoSHTTP - Implementing a DoS attack on a router using Slowloris Script - Performing Distributed DoS attack using HOIC - Detecting and analyzing DoS attack traffic using KFSensor and Wireshark	
10	**Lab 10: Session Hijacking** (*The instructor can choose a lab according to the tools available and time*) - Session hijacking using ZAP (Zed Attack Proxy) - Hijacking a user session using Firebug - Hijacking HTTPS traffic in a network using sslstrip - Performing a MITM attack and Hijacking an established session using websploit	**5**
11	**Lab 11: Evading IDS, Firewalls, and Honeypots :** (*The instructor can choose a lab according to the tools available and time*) - Detecting Intrusions Using Snort - Logging Snort Alerts to Kiwi Syslog Server - Detecting Intruders and Worms using KFSensor Honeypot IDS - HTTP Tunneling Using HTTPort	**3**
12	**Lab 12: Buffer OverFlow :** (*The instructor can choose a lab according to the tools available and time*) - Enumerating Passwords in “Default Password List” - Write a Code - Compile die Code - Execute the Code - Perform Buffer Overflow Attack - Obtain Command Shell	**5**
Textbook	**CEHv9-10 theoretical and practice/Eccouncil**	

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td><b>Information Security Management</b></td><td><b>Course Code</b></td><td colspan="6">CYBR 431</td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR444 & CYBR453</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2"><b>3</b></td><td colspan="2"><b>CTH</b></td><td colspan="2">4</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>2</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

This course covers issues related to administration and management of the security of enterprise information systems and networks. The course includes the following topics: Planning for security, security management models, security management practices, governance, and security policy; threat and vulnerability management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations. The course will study the principles and tools related to these topics. The course will also cover security standards, evaluation, and certification process.

Topics:

- Introduction to Management of Information Security.
- Governance and Strategic Planning for Security.
- Information Security Policy.
- Developing the Security Program.
- Security Management Models
- Security Management Practices
- Personnel And Security

Experiments:

References:

- Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
- **Splunk Enterprise Overview:** **https://docs.splunk.com/Documentation/Splunk/7.2.4/Overview/AboutSplunkEnterprise**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	● **Introduction to Management of Information Security:** ○ What is Management? ▪ Behavioral Types of Leaders ▪ Management Characteristics ▪ Governance ▪ Solving Problems ○ Principles of Information Security Management ▪ Planning ▪ Policy ▪ Programs ▪ Protection ▪ People ▪ Projects	**3**
2	● **Governance and Strategic Planning for Security:** ○ The Role of Planning ▪ Precursors to Planning ○ Strategic Planning ▪ Creating a Strategic Plan ▪ Planning Levels ▪ Planning and the CISO ○ Information Security Governance ▪ The ITGI Approach to Information Security Governance ▪ NCSP Industry Framework for Information Security Governance ▪ CERT Governing for Enterprise Security Implementation ▪ ISO/IEC 27014:2013 Governance of Information Security ▪ Security Convergence ○ Planning for Information Security Implementation ▪ Implementing the Security Program using the SecSDLC	**3**
3	● **Information Security Policy:** ○ Why Policy? ▪ Policy, Standards, and Practices ○ Enterprise Information Security Policy ▪ Integrating an Organization’s Mission and Objectives into the EISP ▪ EISP Elements ▪ Example EISP Elements ○ Issue-Specific Security Policy ▪ Elements of the ISSP ▪ Implementing the ISSP ○ System-Specific Security Policy ▪ Managerial Guidance SysSPs ▪ Technical Specification SysSPs ○ Guidelines for Effective Policy Development and Implementation	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	▪ Developing Information Security Policy ▪ Policy Distribution ▪ Policy Reading ▪ Policy Comprehension ▪ Policy Compliance ▪ Policy Enforcement ▪ Policy Development and Implementation Using the SDLC ▪ Software Support for Policy Administration ▪ Other Approaches to Information Security Policy Development ▪ SP 800-18, Rev. 1: Guide for Developing Security Plans for Federal Information Systems	
4	● **Developing the Security Program:** ○ Organizing for Security ▪ Security in Large Organizations ▪ Security in Medium-Sized Organizations ▪ Security in Small Organizations ○ Placing Information Security Within an Organization ○ Components of the Security Program ○ Information Security Roles And Titles ▪ Chief Information Security Officer ▪ Convergence And The Rise Of The True CSO ▪ Security Managers ▪ Security Administrators And Analysts ▪ Security Technicians ▪ Security Staffers And Watchstanders ▪ Security Consultants ▪ Security Officers And Investigators ▪ Help Desk Personnel ○ Implementing Security Education, Training, And Awareness Programs ▪ Security Education ▪ Security Training ▪ Training Techniques ▪ Security Awareness ○ Project Management In Information Security ▪ Projects Versus Processes ▪ PMBOK Knowledge Areas ▪ Project Management Tools	**3**
5	● **Security Management Models:** ○ Introduction To Blueprints, Frameworks, And Security Models ○ Access Control Models ▪ Categories Of Access Controls ▪ Other Forms Of Access Control ○ Security Architecture Models ▪ Trusted Computing Base ▪ Information Technology System Evaluation Criteria	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	▪ The Common Criteria ○ Academic Access Control Models ▪ Bell-LaPadula Confidentiality Model ▪ Biba Integrity Model ▪ Clark-Wilson Integrity Model ▪ Graham-Denning Access Control Model ▪ Harrison-Ruzzo-Ullman Model ▪ Brewer-Nash Model (Chinese Wall) ○ Other Security Management Models ▪ The ISO 27000 Series ▪ NIST Security Publications ▪ Control Objectives For Information And Related Technology ▪ Committee Of Sponsoring Organizations ▪ Information Technology Infrastructure Library ▪ Information Security Governance Framework	
6	● **Security Management Practices:** ○ Introduction To Security Practices ▪ Benchmarking ▪ Standards Of Due Care/Due Diligence ▪ Selecting Recommended Practices ▪ Limitations To Benchmarking And Recommended Practices ▪ Baselining ▪ Support For Benchmarks And Baselines ○ Performance Measurement In InfoSec Management ▪ InfoSec Performance Management ▪ Building The Performance Measurement Program ▪ Specifying InfoSec Measurements ▪ Collecting InfoSec Measurements ▪ Implementing InfoSec Performance Measurement ▪ Reporting InfoSec Performance Measurements ○ Trends In Certification And Accreditation ▪ NIST SP 800-37, Rev. 1: Guide For Applying The Risk Management Framework To Federal Information System	**3**
7	● **Personnel And Security:** ○ Introduction To Personnel And Security ▪ Staffing The Security Function ▪ Information Security Positions ○ Information Security Professional Credentials ▪ (ISC)2 Certifications ▪ ISACA Certifications ▪ GIAC Certifications ▪ EC-Council Certifications ▪ Comp TIA Certifications ▪ ISFCE Certifications ▪ Certification Costs ▪ Entering The Information Security Profession	**4**

Detailed of Theoretical Contents		
Chapter.	Contents	Hours
	○ Employment Policies And Practices ▪ Hiring ▪ Contracts And Employment ▪ Security As Part Of Performance Evaluation ▪ Termination Issues ▪ Personnel Security Practices ▪ Security Of Personnel And Personal Data ▪ Security Considerations For Temporary Employees, Consultants, And Other Workers	
8	● Protection Mechanisms ○ Introduction To Protection Mechanisms ▪ Access Controls And Biometrics ○ Managing Network Security ▪ Firewalls ▪ Intrusion Detection And Prevention Systems ▪ Remote Access Protection ▪ Wireless Networking Protection ▪ Scanning And Analysis Tools ▪ Managing Server-Based Systems With Logging	**4**
Textbook	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord	

Detailed of Practical, Exercises and Contents		
Chapter.	Contents	Hours
1	**Exercises: Governance and Strategic Planning for Security:** ○ The Role of Planning ○ Strategic Planning ○ Information Security Governance ○ Planning for Information Security Implementation ○ Implementing the Security Program using the SecSDLC	**1**
2	**Exercises: Developing the Security Program:** ○ Organizing for Security ○ Placing Information Security Within an Organization ○ Components of the Security Program ○ Information Security Roles And Titles ○ Implementing Security Education, Training, And Awareness Programs ○ Project Management In Information Security	**2**
3	**Exercises: Security Management Models:** ○ Blueprints, Frameworks, And Security Models ○ Access Control Models ○ Security Architecture Models ○ Academic Access Control Models ○ Other Security Management Models	**2**

	○ Information Security Governance Framework	
4	**Exercises: Security Management Practices:** ○ Concepts in Security Practices ○ Performance Measurement In InfoSec Management ○ Trends In Certification And Accreditation ○ NIST SP 800-37, Rev. 1: Guide For Applying The Risk Management Framework To Federal Information System	**2**
5	**Exercises: Personnel And Security:** ○ Concepts in Personnel And Security ○ Information Security Professional Credentials ○ Employment Policies And Practices	**2**
6	**Lab: Protection Mechanisms: Access Controls And Biometrics**	**3**
7	**Lab: Protection Mechanisms: Managing Network Security** ▪ Scanning And Analysis Tools	**3**
8	**Lab: Protection Mechanisms: Managing Network Security** ▪ Managing Server-Based Systems With Logging (SIEM) ▪ Installation & Configuring of Splunk Enterprise	**3**
9	**Lab: Protection Mechanisms: SIEM** ● Getting Data Into Splunk Enterprise	**3**
10	**Lab: Protection Mechanisms: SIEM** ● Basic Searching in Splunk	**3**
11	**Lab: Protection Mechanisms: SIEM** ● Creating Dashboards in Splunk	**2**
Textbook	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord	

Textbooks	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
	Splunk Enterprise Overview: **https://docs.splunk.com/Documentation/Splunk/7.2.4/Overview/AboutSplunkEnterprise**

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td><b>Digital Forensics</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR424</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR423 and CYBR444</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3"><b>4</b></td><td colspan="2"><b>CTH</b></td><td>6</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>4</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH<b>: Credit Hours</b> L<b>: Lecture</b> P<b>: Practical</b> T<b>: Tutorial</b> CTH<b>: Contact Hours</b></td></tr>
</table>

Course Description:

In this course, students will dive into the bits and bytes to conduct computer, mobile and social forensic investigations; interpret evidence; make inferences; write defensible reports to be used in legal actions; and understand key elements of expert witness testimony. Students will use FTK (Forensic Tool Kit) along with other forensic tools to recover, search, and analyze e-evidence and create reports

Topics:

- Overview of digital investigation and digital evidence
- Data Acquisition of physical storage devices
- Study of file systems with the main focus on Microsoft Windows & Linux Systems
- File System Analysis & file recovery
- File carving & document analysis
- Information hiding & steganography
- Network forensics
- Mobile forensics
- Cloud forensics

Experiments:

Digital forensics tools

References:

- ✓ Hands-on Incident Response and Digital Forensics, Mike Sheward 2018
- ✓ Digital Forensics and Investigations, People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 2018.
- ✓ Digital Forensics with Kali Linu, Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, by Shiva V.N. Parasram. 2017

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**introduction to Computer Forensics:** • Provide general information about digit forensics, • Importance in the investigation of digital crimes. • the steps of forensic investigation	2
2	**Computer forensics:** • Use file types to investigate questionable forensic threats • Investigative Techniques • Linux-based Forensics Analysis • Windows-based Forensics Analysis	3
3	**Anti-Forensics:** Get to know the anti-forensic tools and techniques that are used to hide forensic evidence.	3
4	**Network Forensics:** • Analyze data packets • Digital Crime Scene • Forensics Logs • Investigation of network hacking incidents	5
5	**Mobile Forensics:** • Investigation on mobile devices in order to find forensic evidence • Mobile evidence • Extracting and analyzing mobile evidence	5
6	**Cloud Forensics:** • Forensic evidence in the Cloud computing environment	4
7	**Exploring Memory Forensics:** • Forensic evidence from digital memories.	4

Textbook	✓ **Hands-on Incident Response and Digital Forensics, Mike Sheward 2018** ✓ **Digital Forensics and Investigations, People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 2018.** ✓ **Digital Forensics with Kali Linux, Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, by Shiva V.N. Parasram. 2017**

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab: Building a computer forensics lab:** Create a forensically sound duplicate of the evidence (forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes HDD, SSD, CD/DVD, PDA, mobile phones, GPS, and all tape formats	3
2	**Lab: Linux Forensics** • Collect Volatile and Non-Volatile Information • Use Various Shell Commands • Examine Linux Log files	3
3	**Lab: Windows Forensic Tools:** • Helix3 Pro, X-Ways Forensics, • Windows Forensic Toolchest (WFT), • Autopsy, The Sleuth Kit (TSK),	3
4	**Lab: Data Acquisition Software Tools:** Perform data acquisition (using UltraKit, Active Disk Image, DriveSpy, etc.)	3
5	**Lab: Tools to defeat Anti-Forensics:** (*The instructor can choose a lab according to the tools available and time*) • Use File Recovery Tools (Recover My Files, EaseUS Data Recovery Wizard, etc.), Partition Recovery Tools (Active Partition Recovery, 7-Data Partition Recovery, Acronis Disk Director Suite, etc.), Rainbow Tables Generating Tools (rtgen, Winrtgen), Windows Admin Password Resetting Tools (Active Password Changer, Windows Password Recovery Bootdisk, etc.). • Understand the usage of Application Password Cracking Tools (Passware Kit Forensic, SmartKey Password Recovery Bundle Standard, etc.), Steganography Detection Tools (Gargoyle Investigator™ Forensic Pro, StegSecret, etc.)	5
6	**Lab: Network Forensics Tools:** (*The instructor can choose a lab according to the tools available and time*) • Use network monitoring tools to capture real-time traffic spawned by any running malicious code after identifying intrusion via dynamic analysis • Understand the working of wireless forensic tools (NetStumbler, NetSurveyor, Vistumbler, WirelessMon, Kismet, OmniPeek, CommView for Wi-Fi, WiFi USB Dongle: AirPcap, tcpdump, KisMAC, Aircrack-ng Suite AirMagnet WiFi Analyzer, MiniStumbler, WiFiFoFum, NetworkManager, KWiFiManager, Aironet Wireless LAN	5
7	**Lab: Web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools:** (*The instructor can choose a lab according to the tools available and time*)	5

	Understand the working of web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools (Acunetix Web Vulnerability Scanner, Falcove Web Vulnerability Scanner, Netsparker, N-Stalker Web Application Security Scanner, Sandcat, Wikto, WebWatchBot, OWASP ZAP, dotDefender, IBM AppScan, ServerDefender, Deep Log Analyzer, WebLog Expert, etc.)	
8	**Lab: Malware Forensics Tools:** (*The instructor can choose a lab according to the tools available and time*) Use Malware Analysis Tools (VirusTotal, Autoruns for Windows, RegScanner, MJ Registry Watcher, etc.)	**7**
9	**Lab: Email Forensics Tools:** (*The instructor can choose a lab according to the tools available and time*) Use email forensic tools (Stellar Phoenix Deleted Email Recovery, Recover My Email, Outlook Express Recovery, Zmeil, Quick Recovery for MS Outlook, Email Detective, Email Trace - Email Tracking, R-Mail, FINALeMAIL, eMailTrackerPro, Paraben’s email Examiner, Network Email Examiner by Paraben, DiskInternal’s Outlook Express Repair, Abuse.Net, MailDetective Tool, etc.)	**7**
10	**Lab: Mobile Forensics Software and Hardware Tools:** (*The instructor can choose a lab according to the tools available and time*) Use mobile forensic software tools (Oxygen Forensic Suite, MOBILedit! Forensic, BitPim, SIM Analyzer, SIMCon, SIM Card Data Recovery, Memory Card Data Recovery, Device Seizure, Oxygen Phone Manager II, etc.)	**7**
11	**Lab: Cloud Forensics Tools:** (*The instructor can choose a lab according to the tools available and time*) Use Cloud Forensics Tools (UFED Cloud Analyzer, WhatChanged Portable, WebBrowserPassView, etc.)	**4**

Textbook	✓ **Hands-on Incident Response and Digital Forensics, Mike Sheward 2018** ✓ **Digital Forensics and Investigations, People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 2018.** ✓ **Digital Forensics with Kali Linux, Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, by Shiva V.N. Parasram. 2017**

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td><b>Risk Management & Incident Response</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR 432</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR431</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2"><b>3</b></td><td colspan="2"><b>CTH</b></td><td colspan="2">4</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>2</b></td><td><b>T</b></td><td><b>0</b></td></tr>
</table>

CRH: **Credit Hours** L: **Lecture** P: **Practical** T: **Tutorial** CTH: **Contact Hours**

Course Description :

This course examines information security as a risk management problem where the organization identifies information security risks, evaluates those risks, and makes risk mitigation and acceptance decisions given its resource constraints. In addition, students will learn the concepts and practices of contingency operations, including the administration of the planning process for incident response, disaster recovery, and business continuity planning. Topics include organizational readiness planning, the phases of incident response, different contingency strategies, tasks related to the preparation, implementation, operations, and maintenance of disaster recovery,

Topics :

- Risk Management: Identifying And Assessing Risk.
- Risk Management: Controlling Risk
- Planning for Contingencies
- Incident Response
- Disaster Recovery
- Business Continuity

Experiments:

References :

- Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
- Principles of Incident Response and Disaster Recovery 2nd Edition, by Michael E. Whitman, Herbert J. Mattord, Andrew Green

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	● **Risk Management: Identifying And Assessing Risk:** ○ Introduction To Risk Management ▪ Knowing Yourself ▪ Knowing The Enemy ▪ Accountability For Risk Management ○ Risk Identification ▪ Identification And Prioritization Of Information Assets ▪ Threat Assessment ▪ The TVA Worksheet ○ Risk Assessment And Risk Appetite ▪ Assessing Risk ▪ Likelihood ▪ Assessing Potential Impact On Asset Value (Consequences)	**2**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	▪ Percentage Of Risk Mitigated By Current Controls ▪ Uncertainty ▪ Risk Determination ▪ Likelihood And Consequences ▪ Documenting The Results Of Risk Assessment ▪ Risk Appetite	
2	• **Risk Management: Controlling Risk:** ○ Introduction To Risk Control ▪ Risk Control Strategies ▪ Defense ▪ Transference ▪ Mitigation ▪ Acceptance ▪ Termination ○ Managing Risk ▪ Feasibility And Cost-Benefit Analysis ▪ Other Methods Of Establishing Feasibility ▪ Alternatives To Feasibility Analysis ○ Recommended Risk Control Practices ▪ Qualitative And Hybrid Measures ▪ Delphi Technique ▪ The OCTAVE Methods ▪ Microsoft Risk Management Approach ▪ FAIR ▪ ISO 27005 Standard For InfoSec Risk Management ▪ NIST Risk Management Model ▪ Other Methods ▪ Selecting The Best Risk Management Model	2
3	• **Planning for Organizational Readiness** ○ Introduction to Contingency Planning and Its Components ○ Role of Information Security Policy in Developing Contingency Plans ○ Beginning the Contingency Planning Process ○ Elements Required to Begin Contingency Planning ○ Contingency Planning Policy ○ Business Impact Analysis ○ BIA Data Collection ○ Budgeting for Contingency Operations	2
4	• **Contingency Strategies for IR/DR/BC** ○ Data and Application Resumption ○ Site Resumption Strategies	2
5	• **Incident Response: Planning** ○ The IR Planning Process ○ Developing the Incident Response Policy	2

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	o Incident Response Planning o Assembling and Maintaining the Final IR Plan	
6	• **Incident Response: Detection and Decision Making** o Detecting Incidents o Intrusion Detection and Prevention Systems o Incident Decision Making	**2**
7	• **Incident Response: Organizing and Preparing the CSIRT** o Building the CSIRT o Outsourcing Incident Response	**2**
8	• **Incident Response: Response Strategies** o IR Response Strategies o Incident Containment and Eradication Strategies for Specific Attacks o Automated IR Response Systems	**3**
9	• **Incident Response: Recovery and Maintenance** o Recovery o Maintenance o Incident Forensics o eDiscovery and Anti-Forensics	**3**
10	• **Disaster Recovery: Preparation and Implementation** o Disaster Classifications o Forming the Disaster Recovery Team o Disaster Recovery Planning Functions o Information Technology Contingency Planning Considerations o Sample Disaster Recovery Plans o The DR Plan	**3**
11	• **Disaster Recovery: Operation and Maintenance** o Facing Key Challenges o Preparation: Training the DR Team and the Users o Disaster Response Phase o Recovery Phase o Resumption Phase o Restoration Phase	**3**
Textbook	• Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord • Principles of Incident Response and Disaster Recovery 2nd Edition, by Michael E. Whitman, Herbert J. Mattord, Andrew Green	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**LAB1: Identifying And Assessing Risk (tools for automating risk assessment)** **Exercise 1-6** [Management of Information Security (**chapter6**)]	**2**
2	**LAB2: Controlling Risk (Calculate the SLE, ARO, ALE for threats cases)** **Exercise 1-7** [Management of Information Security (**chapter7**)]	**2**
3	**LAB3: Planning for Organizational Readiness:** In this lab, we will set up a virtual system running Security Onion, an open source intrusion detection, and network monitoring application. We will use Security Onion in future Hands-On Projects, so it’s important to get it set up and running now.	**2**
4	**LAB4: Contingency Strategies for IR/DR/BC** In this lab, we will examine two different ways to make a backup of the Security Onion virtual image we already created. In the first method, we will make a backup from within Security Onion, using command- line tools. In the second method, we will copy the virtual image files themselves.	**2**
5	**LAB5: Incident Response: Planning** In this lab, students will use Security Onion to examine a simulated attack on a network. This exercise will help students understand the basics of how to determine if an attack is taking place, as well as how to get information about the attack so that appropriate action can be taken. Students will use the SQueRT tool in Security Onion to help you analyze data in a meaningful way as well as to examine packets in both individual and session contexts, giving them a deeper understanding of the overall scope of the attack.	**2**
6	**LAB6: Incident Response: Detection and Decision Making** In this lab, students will use the Sguil application in Security Onion to examine another attack on a network. This project will help them understand what was done during an attack by viewing the captured network traffic in a complete session.	**2**
7	**LAB7: Incident Response: Organizing and Preparing the CSIRT** In this lab, students will use Security Onion to examine how an incident can be evaluated to determine where it came from, what malicious software (malware) was downloaded, and what server the malware came from. To do this, students will use the Wireshark application as well as the NetworkMiner application. In this exercise, a user has clicked on a URL in an e-mail, which triggered the malware download.	**2**
9	**LAB8: Incident Response: Response Strategies** In this lab, students will use the Xplico application that’s included in the Security Onion distro to examine a pcap file. Xplico is frequently used to	**3**

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
	enable incident responders to do post-incident forensics work, but it can also be used to examine traffic in real time. Students will simulate an examination of network traffic captured during an incident, looking at the various types of traffic captured in order to determine what the attacker did while on your network.	
9	**LAB9: Incident Response: Recovery and Maintenance** In this lab, students will take a look at chaosreader, a Perl script that is incorporated in the Security Onion distro. Chaosreader is designed to read pcap files and return information on sessions as well as replay some of them. In this lab, students will simulate an examination of network traffic captured during an investigation of suspicious employee activity in order to determine what activities the employee was engaged in while on the network.	**3**
10	**LAB10: Disaster Recovery: Preparation and Implementation** In this lab, we will take a look at Ostinato, an open source packet generator that is incorporated in the Security Onion distro. Ostinato can generate packets of different types and has the added benefit of a user-friendly GUI, as opposed to working strictly from the command line. This lab will walk students through the process of creating a stream of packets using Ostinato, then examining that traffic in Wireshark.	**3**
11	**LAB11: Disaster Recovery: Operation and Maintenance** In this lab, we will take a look at reassembler, a Python script that reassembles fragmented packets in multiple methods so that analysts can view questionable traffic exactly as an IDS saw it, thus helping them determine whether the IDS made a proper decision regarding the traffic in question. Additionally, we will use reassembler to write the traffic to disk, so that binary payloads can be examined in the same form that the potential target operating system would view it.	**3**
Textbook	• Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord • Principles of Incident Response and Disaster Recovery 2nd Edition, by Michael E. Whitman, Herbert J. Mattord, Andrew Green	

Textbooks	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
	Principles of Incident Response and Disaster Recovery 2nd Edition, by Michael E. Whitman, Herbert J. Mattord, Andrew Green

<table>
<tr><td><b>Department</b></td><td>Computer Engineering and Information Technologies</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td>Ethics and Cyber Law</td><td><b>Course Code</b></td><td colspan="6">CYBR461</td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR 423</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="2">2</td><td colspan="2">CTH</td><td colspan="2">2</td></tr>
<tr><td>L</td><td>2</td><td>P</td><td>0</td><td>T</td><td>0</td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

This course provides students with the required knowledge and skills to read and understand the legal aspects of any information system. In this course, students will learn cyber law and cybercrimes. Later in the course, students will master the basics of data protection and intellectual property.
`

Topics:

- Understanding Saudi Anti-cybercrime law
- Understanding intellectual property and copyrights
- Understanding the confidence law
- Understanding Trademarks
- Information technology contracts
- Information communication frauds

Experiments:

References:

- Introduction to information technology law 6th edition.

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Introduction to ethics and cyber law** • Saudi Anti-cybercrime law	1
2	**Introduction to intellectual property rights** • Copyright law • The law of confidence • Patent law • Trademarks and passing off • The law relating to designs • Semiconductor Regulations	1
3	**Basic principles of copyright** • Copyright works • Owners and authors • Duration of copyright • The acts restricted by copyright • Infringement • Exceptions to infringement and the permitted acts • Secondary infringement and criminal offences • Remedies for infringement • Copy protection and electronic rights management information • Moral rights	2

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	• Dealing with copyright	
4	**Copyright and computer programs** • Historical development of copyright for computer programs • Subsistence of copyright in computer programs • Preparatory design material for computer programs • Restricted acts for computer programs • Permitted acts for computer programs • Programming languages and instruction sets • Ownership, employees and freelance programmers • Open source software and copyright • Copyright databases in the UK before 1 January 1998 • The US and the ‘sweat of the brow’ principle • Protection of databases in the UK and Europe • Copyright databases • The database right	2
5	**Copyright in the information society** • Introduction • The internet • Multimedia • Legal liability of internet service providers • Circumvention of ‘copy-protection’ • Electronic rights management information	2
6	**The law of confidence** • Basic requirements • viii Contents • Public interest and freedom of expression • Remedies for breach of confidence • Court orders and breach of confidence	2
7	**Trademarks, passing off and malicious falsehood** • Introduction • Trademarks • Trademarks and the internet • Passing off • Malicious falsehood	2
8	**Fundamentals of information technology contracts** • Terms of the contract • Entire agreement • Nature of the contract • Software acquisition • Hardware acquisition • Breach of contract • Misrepresentation	2

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
9	**Liability for defective hardware or software** • Negligence • Negligence and RSI • Negligent misstatement • Product liability • Criminal liability for defective products • Exemption Clauses	1
9	**Outsourcing contracts** • Definitions • Outsourcing company's obligations • Client's obligations • Employment obligations • Duration of contract • Payment • Service change • Warranties • Performance monitoring • Specially written software • Contents • Contents xi • Privacy and data protection law • Further terms in outsourcing contracts	2
10	**Information and communications technology fraud** • Basics of English criminal law • The computer as an unwitting accomplice • The old deception offences • The Fraud Act 2006 • Conspiracy to defraud • The law of attempts • ICT fraud as theft	2
11	**Unauthorized access to computer material** • The problem in perspective • Employment law and unauthorized access • The case of R v Gold • The basic unauthorized access offence • The ulterior intent offence • Jurisdiction • Communications offences • Other offences associated with hacking	2
12	**Computer pornography, harassment, and incitement** • Pornography • Sentencing for child pornography • Sexual grooming of children by e-mail or in chat-rooms • Threatening e-mails	2

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
	• Incitement	
13	**Data protection and freedom of information** • Introduction to data protection law • The data protection Directive • The Data Protection Act 1998 • The data protection principles • Definitions • Role of the Information Commissioner • The Information Tribunal and appeals • The Working Party • xiv Contents	2
14	**Privacy in electronic communications** • Introduction • The Directive on privacy and electronic communications • Specific aspects of the Regulations	1
Textbook	• Introduction to information technology law 6th edition.	

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td><b>Trusted computing</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR 471</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR322, INSA444</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3">3</td><td colspan="2"><b>CTH</b></td><td>4</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>2</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH<b>: Credit Hours</b> L<b>: Lecture</b> P<b>: Practical</b> T<b>: Tutorial</b> CTH<b>: Contact Hours</b></td></tr>
</table>

Course Description:

This course is an introduction to the fundamental technologies behind Trusted Computing, including machine authentication, data protection, attestation, data backup, and system maintenance, etc. The course will also introduce students to the various software resources that exist today to support TPMs (Trusted Platform Modules) and what capabilities they can provide both at an in-depth technical level and in an enterprise context.

Students will also learn about how other technologies such as the Dynamic Root of Trust for Measurement (DRTM) and virtualization can both take advantage of TPMs

The course provides in-depth knowledge on trust computing in networks

1. To learn the concepts of trust categories
2. To understand trust architecture and formalization of security properties
3. To learn trusted computing and administration

Topics:

- Be able to explain critically the notion of trust as embodied in trusted computing devices, and the requirements upon those devices;
- Know the role and purpose of each element of the trusted platform module;
- Be able to use the Trusted Software Stack API to interact with the TPM;
- Understand how technologies of virtualization can combine with trusted platform modules to yield trusted infrastructure;
- Describe some systems architectures which use these capabilities to provide innovative and strong security solutions.

Experiments:

References :

- ✓ A practical guide to trusted computing / David Challener, Kent Yoder.
- ✓ Trusted Computing Platforms, Design and Application, by Smith, Sean 2005
- ✓ Trusted Computing, Principles and Applications, by Tsinghua University Press 2018

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Trusted Computing and secure identification** • Administration of trusted devices. • Secure /backup maintenance • assignment of key certificates-secure time reporting-key recovery	**2**
2	**Trusted Computing and Multilevel Security** • The Bell-LaPadula Model for Computer Security • Other Formal Models for Computer Security	**3**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	• The Concept of Trusted Systems • Application of Multilevel Security	
3	**Trust and Security** • Trust as predictable behavior; • role of the elements of a trusted infrastructure; • objections to this architecture; • potential for good and bad outcomes; • limitations of this approach.	2
4	**Roots of Trust** • The TPM and its place in establishing roots of trust for storage, • measurement, and reporting (identity) on the platform.	3
5	**TPM** • The design of the TPM and its behavior; • the standard APIs for addressing these capabilities; • the Trusted Software Stack.	3
6	**Chain of Trust** • The place of third parties in assuring trusted platforms; • trusted boot processes; • trusted applications.	3
7	**Trusted Virtualization** • Whole system virtualization; • virtual machine managers/hypervisors; • use of trusted platforms to assure virtual machines; • virtual trusted platforms.	4
8	**Applications** • Trusted Boot; • Trusted Network Connect; • Trusted Grid.	2
9	**Mobile Platforms** • Trusted mobile platforms; • additional roots of trust; • suitable architectures for mobile applications	4
Textbook	✓ A practical guide to trusted computing / David Challener, Kent Yoder. ✓ Trusted Computing Platforms, Design and Application, by Smith, Sean 2005 ✓ Trusted Computing, Principles and Applications, by Tsinghua University Press 2018	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab: implement symmetric cryptography algorithm**	**2**
2	**Lab: implement asymmetric cryptography algorithm**	**2**
3	**Lab: TPM provisioning** • Turning on the TPM • The Endorsement Key: Theory vs. Reality • Provisioning TPM Keys	**3**
4	**Lab: Using the TPM: Machine Authentication and Attestation** • PCRs and Locality • Attestation • Machine authentication	**5**
5	**Lab: Using the TPM: Data Protection and Storage** • Using Storage Keys • Using Binding Keys • NVRAM	**6**
6	**Lab: Using the TPM: Other TPM Features**	**4**
7	**Lab: Programming for the TPM and other practical topics**	**4**
Textbook	✓ A practical guide to trusted computing / David Challener, Kent Yoder. ✓ Trusted Computing Platforms, Design and Application, by Smith, Sean 2005 ✓ Trusted Computing, Principles and Applications, by Tsinghua University Press 2018	

Department	Engineering of Computer and Information Technology	**Major**	Cyber Security					
Course Name	Embedded System Security	**Course Code**	**CYBR472**					
Prerequisites	CYBR322, CYBR352	**Credit Hours CRH**	**3**		**CTH**		**4**	
			L	**2**	**P**	**2**	**T**	**0**
CRH**: Credit Hours**	L**: Lecture**	P**: Practical**	T**: Tutorial**	CTH**: Contact Hours**				

Course Description :

The course Study of various security models and techniques for embedded systems both from a hardware as well as a software perspective. Smart card security. RFID attack models (including power analysis, side channel, and timing attacks), and security techniques. Security in wireless sensor networks (key management techniques, attack models, detection and prevention techniques). eHealth (embedded medical systems) security. Cryptographic hardware. Industrial control systems (SCADA). Physical hardware. Security for System-on-chip, and Internet-devices such as Internet thermostats and automated doors.

Topics :

At the end of the unit student will be able to understand:

- ✓ What are embedded software characteristics,
- ✓ implementation and security application of embedded systems.
- ✓ Architecture for embedded systems security
- ✓ Implementing hardware and software security in Embedded systems.

Experiments:

- FPGA Programmer
- EPROM Programmer
- Microcontroller

References :

- ✓ Embedded Systems Security, Practical Methods for Safe and Secure Software and Systems Development; David Kleidermacher Mike Kleidermacher 2012.
- ✓ Hands-On Embedded System Design, Leverage the power of ARM Processors, FPGAs, ASIPs and ASICs for building effective embedded system design 2018.

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**Chapter 1: Introduction to embedded systems security** • What is an Embedded System? • Embedded Systems fundamentals • Embedded Systems Attacks • Uniquely Embedded Concerns • Reliability and Security • Obscurity and Security	**4**
2	**Chapter 2: Systems Software Considerations** • Core Embedded Operating System Security Requirements • Access Control and Capabilities	**4**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	• I/O Virtualization • Assuring Integrity of the TCB	
3	**Chapter 3: Defenses in Software** • Common Firmware Vulnerabilities • Defensive Software Architectures • Combating Complexity • Secure RTOS • Memory Partitioning and Protection • CPU Time Partitioning • Locking Down Firmware	**3**
4	**Chapter 4: Defenses in Hardware** • Securing External Memory • JTAG/Debug Port Considerations • Other Physical Attack Vectors • Tamper Detection and Logging • Exception Handling • Race Conditions • User Interface • Case Study: A/D Converters • FPGAs and Security	**3**
5	**Chapter 5: Secure Embedded Software Development** • Principles of High-Assurance Software Engineering • Embedded Software Security Principles and Patterns • Secure Development Process • Architectural Design Patterns for Embedded Software Security • Model-Driven Design	**6**
6	**Chapter 6:** Practical Methods for Embedded Software Security • Overview of Cryptography for Embedded Software • Embedded System-Level Security • Update on Static Code Analysis for Embedded Software Security • Metrics for Software Defects and Vulnerabilities	**6**

Textbook	• Embedded Systems Security, Practical Methods for Safe and Secure Software and Systems Development; David Kleidermacher Mike Kleidermacher 2012. • Hands-On Embedded System Design, Leverage the power of ARM Processors, FPGAs, ASIPs and ASICs for building effective embedded system design 2018.

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab1: introduction to FPGA**	**1**
2	**Lab2: Implementing Application witch FPGA**	**3**

3	**Lab3: Implementing Symmetric encryption witch FPGA**	**3**
4	**Lab4: Implementing Asymmetric encryption witch FPGA**	**2**
5	**Lab5: Implementing Authentication procedures witch FPGA**	**3**
6	**Lab6: Implementing hardware security over real system**	**7**
7	**Lab7: Implementing software security over the real system.**	**7**
Textbook	• Embedded Systems Security, Practical Methods for Safe and Secure Software and Systems Development; David Kleidermacher Mike Kleidermacher 2012. ● Hands-On Embedded System Design, Leverage the power of ARM Processors, FPGAs, ASIPs and ASICs for building effective embedded system design 2018.	

<table>
<tr><td><b>Department</b></td><td>Engineering of Computer and Information Technology</td><td><b>Major</b></td><td colspan="6">Cyber Security</td></tr>
<tr><td><b>Course Name</b></td><td><b>Internet of Things Security</b></td><td><b>Course Code</b></td><td colspan="6"><b>CYBR481</b></td></tr>
<tr><td rowspan="2"><b>Prerequisites</b></td><td rowspan="2">CYBR441</td><td rowspan="2"><b>Credit Hours CRH</b></td><td colspan="3"><b>3</b></td><td colspan="2"><b>CTH</b></td><td>4</td></tr>
<tr><td><b>L</b></td><td><b>2</b></td><td><b>P</b></td><td><b>2</b></td><td><b>T</b></td><td><b>0</b></td></tr>
<tr><td colspan="9">CRH: <b>Credit Hours</b> L: <b>Lecture</b> P: <b>Practical</b> T: <b>Tutorial</b> CTH: <b>Contact Hours</b></td></tr>
</table>

Course Description:

"Internet of Things" (IoT) is an emerging technology that is changing our world with its innovative products such as "smart homes", "consumer wearables", and "autonomous vehicles". This course aims to introduce the concept of IoT and its impact on our daily lives, to understand the architecture and components of IoT, and to address the challenges and solutions of deploying IoT in reality. Students will learn how to make design trade-offs between communication and computation costs and between hardware and software. In addition, cybersecurity is a critical design issue of the IoT system. From this course, students will become aware of the cybersecurity issues raised by IoT and gain knowledge of the related security techniques. Students will also gain hands-on experiences in building IoT devices and implementing security techniques through team projects.

Topics:

Students successfully completing this course will:

- Understand the impact of IoT technologies
- Be able to draw the big picture of the IoT ecosystem
- Be able to identify the architecture of IoT systems
- Be able to describe the essential components of IoT
- Have the knowledge of the emerging technologies of IoT
- Be able to examine the security and privacy challenges of IoT
- Be able to find appropriate security/privacy solutions for IoT
- Have hands-on experience in IoT and security projects.

Experiments:

Raspberry PI
Arduino

References:

✓ IoT fundamentals, Cisco Networking Academy,
✓ IoT Security: Practical guide book, 2016, by David Etter
✓ Practical Internet of Things Security, by Drew Van Duren, Brian Russell, Publisher: Packt Publishing June 2016

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
1	**IoT Technology Standards** • Introduction to IOT • Sensors and Nodes used in IoT • Data Analytics in IoT • Wired Communication Protocols (UART, USART, I2C, SPI, Ethernet, JTAG) • Wireless Communication Protocols (Bluetooth, Zigbee, 6lowPAN, WiFi, Z-wave)	**2**
2	**IoT Architecture** • Device To Device • Device To Cloud • Device To Gateway • Cloud To Gateway • Sensors and actuators in IoT	**3**
3	**IoT Communication Protocol** • Application Layer Protocols (MQTT, CoAP, HTTP, Web socket, DDS, AMQP) • Transport Layer Protocols (TCP, UDP) • Network Layer Protocols (IPv4, IPv6, LowPAN) • Link Layer Protocols (Ethernet, WiFi, WiMax, Cellular)	**3**
4	**Introduction to Raspberry PI** • Understanding Raspberry PI • Setting up Raspberry PI • Installation of OS in Raspberry PI (Noobs and Kali Linux) • Setting remote access to Raspberry PI Desktop	**2**
5	**Exploring of Arduino ide** • Learning fundamentals and programming on Arduino IDE • Interfacing Sensors and Peripherals with Arduino • Developing Internet of Things Prototypes	**2**
6	**The need of Internet of Things (IoT) Security** • Requirements and Basic Properties • Main Challenges • Main Security Issues • Confidentiality, Integrity, Availability • Non-Repudiation	**3**
7	**Security Classification & Access Control** • Data Classification (Public, Private, Sensitive, Confidential, Proprietary) • Criteria for Data Classification • Privacy Issues in IoT • IoT Ecosystem Access Control • Authentication, Authorization, Accounting	**2**

Detailed of Theoretical Contents		
Chapter.	**Contents**	**Hours**
	• Data Integrity	
8	**Attack Surface and Threat Assessment** • OWASP Top 10 (IoT Hacking & Security) • IoT Attack Surface • Software and Cloud Components • Firmware of the devices • Web Application Dashboard • Mobile Application used to Control, Configure, and Monitor Devices • Threat Assessment	**3**
9	**Attacks & Implementation** • Risk of IoT • Vulnerability Exploitation • Attacks of Privacy (Phishing, Pharming, DNS Hijacking, Defacement, Eavesdropping, Cyber Espionage) • Web-Based Attacks (Malware, Password, Access, Social Engineering, Data & Identity Theft, Reconnaissance)	**2**
10	**Case Studies and Discussion** • Smart Homes • Smart Agriculture • Smart Retail Supply • Smart Healthcare • Smart Grid • Smart Cities	**4**
Textbook	✓ IoT fundamentals, Cisco Networking Academy, ✓ IoT Security: Practical guide book, 2016, by David Etter ✓ Practical Internet of Things Security, by Drew Van Duren, Brian Russell, Publisher: Packt Publishing June 2016	

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
1	**Lab1:** Introduction to Arduino and hands-on	**1**
2	**Lab 2:** Introduction Raspberry PI and hands-on	**1**
3	**Lab 3:** Setup different sensors and input devices and obtain the readings via Arduino or Raspberry PI	**1**
4	**Lab 4:** Setup ad-hoc network between IoT devices	**1**
5	**Lab 5:** Setup wireless communication between IoT devices and cloud servers	**2**

Detailed of Practical Contents		
Chapter.	**Contents**	**Hours**
6	**Lab 6:** Analyze multiple sensors data and trigger events	**3**
7	**Lab 7:** Analyze the traffic between IoT devices	**2**
8	**Lab 8:** Implement encryption in IOT devices	**2**
9	**Lab 9:** Implement integrity feature in IoT devices	**2**
10	**Lab 10:** Implement a Privacy preserving IoT scheme	**2**
11	**Lab 11:** Implement a technique to sink data acknowledgment for a device and deplete its battery	**2**
12	**Lab 12:** Implement a technique to change data send by the device to change data to trigger alarm	**2**
13	**Lab 13:** Implement a technique to change data for the device to behave abnormally	**2**
14	**Lab 14:** Implement a technique to manage and detect data manipulation in the traffic	**3**

Textbook	✓ IoT fundamentals, Cisco Networking Academy, ✓ IoT Security: Practical guide book, 2016, by David Etter ✓ Practical Internet of Things Security, by Drew Van Duren, Brian Russell, Publisher: Packt Publishing June 2016 ✓ Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, by Francis daCosta ✓ IoT Security Issues, by Alasdair Gilchrist

Department	Computer Engineering and Information Technologies	**Major**	Cyber Security					
Course Name	Advanced Security Topics	**Course Code**	CYBR482					
Prerequisites	CYBR444, CYBR453	**Credit Hours CRH**	3		CTH		4	
			L	2	P	2	T	0

CRH: **Credit Hours** L: **Lecture** P: **Practical** T: **Tutorial** CTH: **Contact Hours**

Course Description:

Advanced topics in cyber security focus on the emerging fields in cyber security. Apart from traditional concepts, this course focuses on emerging information technology fields where a great deal of research is being done and a potential of more research is there. The course covers the most recent topics such as Block chain, Artificial Intelligence, Machine learning, Cryptocurrency, etc. From this course, students will have an overview of the most recent cyber security topics

Topics:

- Blockchain technology and achieving transactional security
- AI based cyber security algorithms
- Machine learning
- New and recent topics in cyber security

Experiments:

References:

- Machine Learning and Security, Protecting Systems with Data and Algorithms, by Clarence Chio, David Freeman, 2018.
- An Introduction to Ethereum and Smart Contracts by Sebastián E. Peyrott
- Bitcoin: A Peer-to-Peer Electronic Cash System
- Understanding Machine Learning: From Theory to Algorithms, by Shai Shalev-Shwartz and Shai Ben-David 2014.
- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher 2017.

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**Chapter 1: Blockchain Concept and building model** • Theory • Protocols • Bitcoin • Ethereum • Mining and Cryptocurrencies • Types of Blockchain and Enterprise	6
2	**Chapter 2: Block chain Application in Cyber Security – Case Study** • Security and Safeguards • Protection from attackers • Hacks on exchanges • What is stopping adoption? • Scalability problems • Network attacks to destroy bitcoin • Case Studies	3

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
3	**Chapter 3: Introduction to Artificial Intelligence (AI)** • Concepts • Types and models • Algorithms and techniques used	6
4	**Chapter 4: AI based applications** • Threat Monitoring • User behavior analysis • Case studies	3
5	**Chapter 5: Introduction to machine learning** • Theory/classification • Different algorithms used in ML	4
6	**Chapter 6: Machine learning advancements in recent times** • ML for cybersecurity • ML in IoT • Case studies	4
Textbook	• Machine Learning and Security, Protecting Systems with Data and Algorithms, by Clarence Chio, David Freeman, 2018. • Artificial Intelligence, A modern approach By Peter Norvig And Stuart Russell 2010. • Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher 2017. • Understanding Machine Learning: From Theory to Algorithms, by Shai Shalev-Shwartz and Shai Ben-David 2014.	

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**Lab 1:** • Set up Hyper ledger Fabric	2
2	**Lab 2:** • Set up Hyper ledger Explorer	2
3	**Lab 3:** • Set up Hyper ledger Composer	2
4	**Lab 4:** • Set up Hyper ledger Composer playground	3
5	**Lab 5:** • Transfer assets in a block chain network	3
6	**Lab 6:** • Implementing AI application (Pattern recognition, Decision,…)	2
7	**Lab 7:** • Implementing security solution managed by AI application	3

Detailed of Practical Contents		
No.	**Contents**	**Hours**
8	**Lab 8:** • Experience Machine Learning Tools ○ TensorFlow	2
9	**Lab 9:** • Implement Matrices based User Behavior Classification using TensorFlow	3
10	**Lab 10:** • Use ML to secure a network	4
Textbook	• An Introduction to Ethereum and Smart Contracts by Sebastián E. Peyrott • Bitcoin: A Peer-to-Peer Electronic Cash System • Machine Learning and Security, Protecting Systems with Data and Algorithms, by Clarence Chio, David Freeman, 2018.	

Department	Engineering of Computer and Information Technology	**Major**	Cyber Security					
Course Name	**Graduation Project**	**Course Code**	**CYBR 491**					
Prerequisites	CYBR 423, CYBR 431, CYBR 442	**Credit Hours** **CRH**	4		**CTH**		6	
			L	2	**P**	4	**T**	0

CRH: **Credit Hours** L: **Lecture** P: **Practical** T: **Tutorial** CTH: **Contact Hours**

Course Description:

The trainee should choose a topic that reflects the knowledge and skills he learned throughout the program study. It is recommended that each student does his own project. The project-based learning method should be conducted in this course.

Topics:

- Week 1-2: Forming the team, selecting a project topic, and studying the final report format.
- Week 3: project proposal approval by the advisor.
- Week 4: Project plan due.
- Week 5-8: Start building/implementing the project and advisor feedback.
- Week 9: Progress report and presentation and advisor feedback.
- Week 10-13: Building project continue and start writing the final report.
- Week 14: Testing or/and Debugging or/and Troubleshooting.
- Week 15: Distributing the final report to the testing committee.
- Week 16: The final report and presentation in front of the committee.

Experiments:

References :

Appendix

Appendix Laboratory Equipment, Workshops and Laboratories

No.	Laboratory name/workshop	Capacity of training	Human Resources	Training courses benefiting from the laboratory/workshop/ lab
1	Cyber Security Lab	20	Appendix 4	• Operating Systems Security • Fundamentals of Cyber Security • Penetration Testing • Digital Forensics • Information Security Management • Risk Management & Incident Response
2	Networking Lab	20	Appendix 4	• Computer Networks • Basic Networks Systems Administration • Open Source Network Systems
3	Programming Lab	20	Appendix 4	• Foundation of Computer Programming • Advanced Programming • Secure Software Development • Trusted Computing • Embedded Systems Security
4	Network Security Lab	20	Appendix 4	• Networks & Communications Security • Advanced Technologies in Networks Security • Wireless Networks Security • Cloud Computing & Virtualization Security

Appendix 1

List of Detailed Equipment for Two Cybersecurity Laboratories, In addition to Networking and programming labs.

Security Lab		
No.	**Hardware Specifications**	**Quantity**
1.	• HP EliteOne 800 G3 23" Touch all-in-One (Y8C76AV) Intel® Core 17-7700 Processor (3.6 GHz, up to 4.2 GHz w/Turbo Boost, 8MB cache, 4 cores) + Intel® HD Graphics 630,32 GB DDR4 Memory, 1TB 7200 RPM SATA HDD, 256 GB SSD. • USB Wi-Fi card that can support packet injection and packet sniffing, recommended ALFA card from ALFA Networks • Bluetooth USB Dongle Adapter.	40
2.	• HP EliteOne 800 G3 23" Touch all-in-One (Y8C76AV) Intel® Core 17-7700 Processor (3.6 GHz, up to 4.2 GHz w/Turbo Boost, 8MB cache, 4 cores) + Intel® HD Graphics 630,32 GB DDR4 Memory, 1TB 7200 RPM SATA HDD, 512 GB SSD. • USB Wi-Fi card that can support packet injection and packet sniffing, recommended ALFA card from ALFA Networks • Bluetooth USB Dongle Adapter.	2
3.	Cisco ASA 5508-X w/ FirePOWER Services, Software Image for This ASA, Image should be managed directly through ASDM and CLI.	2
4.	Palo Alto PA 220 Next-generation firewall in a small footprint, with last PAN-OS image.	2
5.	Fortigate/FortWiFi 30E, for Enterprise Branch, Secure SD-WAN with UTM, Last FortiOS image.	2
6.	Sophos FirewallXG 85 / 85w Rev.3 desktop models, with WiFi, Latest ios image.	2
7.	Cisco 7600 Wireless Security Gateway R4.	2
8.	Cisco Aironet 700W Series Access Points	2
9.	Cisco 3504 Wireless Controller	2

Appendix 2

No.	Software Programs	Quantity
1.	IBM QRadar Security intelligence Platform.	20
2.	Risk management software	20
3.	Nessus Pro	20
4.	SANS investigative Forensics Toolkit (SIFT)	20
5.	Encase Forensic or X-Way Forensics.	20
6.	MATLAB software	20

Appendix 3

Instructors Qualifications requirements

No.	Course Code	Course name	Instructor Qualifications
1	CYBR 312	Operating Systems Security	**Master/PH.D. in Information Security related fields Or IT related + (GCWN or GCUX or equivalent)**
2	CYBR 321	Fundamentals of Cyber Security	**Master/PH.D. in Information Security related fields or IT related +(GSEC or equivalent)**
3	CYBR 322	Applied Cryptography	**Master/PH.D. in Information Security related fields Or IT related + (ECES or CECP or equivalent)**
4	CYBR 351	Foundation of Computer Programming	**Master/PH.D. in Computer Science or IT Related fields**
5	CYBR 352	Advanced Programming	**Master/PH.D. in Computer Science or IT Related fields**
6	CYBR 453	Secure Software Development	**Master/PH.D. in Computer Science + (CSSLP or GSSP or equivalent)**
7	CYBR 441	Networks & Communications Security	**Master/PH.D. in Information Security related fields Or Networking related fields + (CND or equivalent)**
8	CYBR 442	Advanced Technologies in Networks Security	**Master/PH.D. in Information Security related fields or IT related +(GNFA or [EC-council CAST 614] or CCNP Security Specialization or equivalent)**
9	CYBR 443	Wireless Networks Security	**Master/PH.D. in Information Security related fields or IT related + (GAWN or OSWP or CWSP equivalent)**
10	CYBR 444	Cloud Computing & Virtualization Security	**Master/PH.D. in Information Security related fields or IT related +(CCSP or CCSS or CCSK or equivalent)**

11	CYBR 423	Penetration Testing	**Master/PH.D. in Information Security related fields** **Or IT related +(GPEN or LPT or OSCP or equivalent)**
12	CYBR 424	Digital Forensics	**Master/PH.D. in Information Security related fields** **or IT related +** **(GCFE or GCFA or CCFE or CHFI or equivalent)**
13	CYBR 431	Information Security Management	**Master/PH.D. in Information Security related fields** **or IT related +** **CISSP or CISM or GISP or C|CISO or CISA or equivalent**
14	CYBR 432	Risk Management & Incident Response	**Master/PH.D. in Information Security related fields** **or IT related + (GCIH or CGEIT or CRISC or equivalent)**
15	CYBR 461	Ethics and Cyber Law	**Master/PH.D. in any IT related fields**
16	CYBR 471	Trusted Computing	**Master/PH.D. in Information Security related fields**
17	CYBR 472	Embedded Systems Security	**Master/PH.D. in Information Security related fields** **Or Computer Engineering**
18	CYBR 481	Internet of Things Security	**Master/PH.D. in Information Security related fields**
19	CYBR 482	Advanced Security Topics	**Master/PH.D. in Information Security related fields** **Or** **Any Curriculum courses instructor qualifications'**
20	CYBR 491	Graduation Project	**Master/PH.D. in Information Security related fields** **Or** **Any Curriculum courses instructor qualifications'**
21	MATH304	Applied Mathematics	**Master or PH.D. in Applied Mathematics only**
22	INET 313	Computer Networks	**Master or PH.D. in Networking Technologies related fields.**
23	INSA 312	Basic Networks Systems Administration	**Master or PH.D. in Network Technologies related fields.**
24	INSA 444	Open Source Network Systems	**Master or PH.D. in Network Technologies related fields.**

Appendix 4

References

Textbooks	1.	Pfleeger, C.P., Security in Computing 5th Edition, Prentice Hall.
	2.	Cryptography and Network Security by William Stalling, 2011
	3.	Trent Jaeger: Operating System Security
	4.	Andrew S. Tanenbaum: Modern Operating Systems
	5.	Cryptography and Network Security: Principles and Practice, William Stallings, 7 Edition, 2017
	6.	Starting Out with Python
	7.	How to Think Like a Computer Scientist: Learning with Python 3
	8.	Web Programming Step by Step, 2nd Edition, by Stepp/Kirst/Miller
	9.	Web Programming and Internet Technologies, 2nd Edition by Scobey
	10.	Official (ISC)2 Guide to the CSSLP CBK ((ISC)2 Press) 2nd Edition by Mano Paul
	11.	Core Software Security by James Ransome and Anmol Misra
	12.	OWASP WebGoat Project, https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
	13.	CCNA Security, Cisco Networking Academy,
	14.	Security of Information and Communication Networks, by Stamatios V. Kartalopoulos, 2009
	15.	Network Security: Data and Voice Communications (McGraw-Hill Series on Computer Communications), 1995
	16.	CCNP Security: • Implementing Cisco Secure Access Solutions (SISAS) • Implementing Cisco Edge Network Security Solutions (SENSS) • Implementing Cisco Secure Mobility Solutions (SIMOS) • Implementing Cisco Threat Control Solutions (SITCS)
	17.	LTE Security, John Wiley & Sons, 2010. Edney, Arbaugh
	18.	Real 802.11 Security, Addison-Wesley 2004
	19.	Wireless and Mobile Network Security, Chaouchi, Hakima, 2009. Pub: John Wiley & Sons Inc
	20.	Advanced penetration testing, Wil Allsopp, Publisher Wiley 2016
	21.	Barrie Sosinsky. 2011. Cloud Computing Bible (1st ed.). Wiley Publishing.
	22.	CEHv9-10 theoretical and practice/ECCouncil

	23.	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
	24.	**Splunk Enterprise Overview:** **https://docs.splunk.com/Documentation/Splunk/7.2.4/Overview/AboutSplunkEnterprise**
	25.	Hands-on Incident Response and Digital Forensics, Mike Sheward 2018
	26.	**Digital Forensics and Investigations, People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 2018.**
	27.	**Digital Forensics with Kali Linux, Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, by Shiva V.N. Parasram. 2017**
	28.	Management of Information Security, 5th Edition by Michael E. Whitman; Herbert J. Mattord
	29.	Principles of Incident Response and Disaster Recovery 2nd Edition, by Michael E. Whitman, Herbert J. Mattord, Andrew Green
	30.	Introduction to information technology law 6th edition.
	31.	A practical guide to trusted computing / David Challener, Kent Yoder.
	32.	Trusted Computing Platforms, Design and Application, by Smith, Sean 2005
	33.	Trusted Computing, Principles and Applications, by Tsinghua University Press 2018
	34.	Embedded Systems Security, Practical Methods for Safe and Secure Software and Systems Development; David Kleidermacher Mike Kleidermacher 2012.
	35.	Hands-On Embedded System Design, Leverage the power of ARM Processors, FPGAs, ASIPs and ASICs for building effective embedded system design 2018.
	36.	IoT fundamentals, Cisco Networking Academy.
	37.	IoT Security: Practical guide book, 2016, by David Etter
	38.	Practical Internet of Things Security, by Drew Van Duren, Brian Russell, Publisher: Packt Publishing June 2016
	39.	Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, by Francis DaCosta
	40.	IoT Security Issues, by Alasdair Gilchrist
	41.	Machine Learning and Security, Protecting Systems with Data and Algorithms, by Clarence Chio, David Freeman, 2018.
	42.	An Introduction to Ethereum and Smart Contracts by Sebastián E. Peyrott
	43.	Bitcoin: A Peer-to-Peer Electronic Cash System
	44.	Understanding Machine Learning: From Theory to Algorithms, by Shai Shalev-Shwartz and Shai Ben-David 2014.
	45.	Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher 2017.
	46.	Machine Learning and Security, Protecting Systems with Data and Algorithms, by Clarence Chio, David Freeman, 2018.

Appendix 5