The Hashemite University

الجامعـــــة الهاشميـــــة

Deanship of Academic Development and International Outreach

عمادة التطوير الأكاديمي والتواصل الدولي

Syllabus: Cyber Defense Monitoring (2010021742)

Second Semester 2021/2022

COURSE INFORMATION

Course Name: Cyber Defense Monitoring **Semester:** Second Semester 2021 /2022 **Department:** Department of CIS **Faculty:** Prince Al-Hussein bin Abdullah II Faculty for Information Technology	**Course Code:** 2010021731 **Section:** 1 **Core Curriculum**:
Day(s) and Time(s): Thursday: 13:00-16:00 **Classroom:** IT: 302	**Credit Hours:** 3 **Prerequisites**: None

COURSE DESCRIPTION

This course concentrates on a number of important Cyber Defense Monitoring techniques and solutions. The course focuses on event logging and collection with syslog protocol, regular expression language and its applications to system/network monitoring, event correlation, and finally network intrusion detection and prevention. The course also discusses a number of open source monitoring solutions, including UNIX rsyslog package, Simple Event Correlator, and Snort IDS/IPS.

DELIVERY METHODS

The course will be delivered through a combination of active learning strategies. These will include:

- PowerPoint lectures and active classroom-based discussion
- Course Project
- E-learning resources: e-reading assignments through Model and Microsoft Team

FACULTY INFORMATION

Name	**Ibrahim MOh'd Salem Obeidat**
Academic Title:	**Professor**
Office Location:	**IT 226**
Telephone Number:	**4773**
Email Address:	**imsobeidat@hu.edu.jo**
Office Hours:	**Monday** 1.00-2.00 / **Wednesday** 1.00-2.00 *Please send an e-mail (imsobeidat@hu.edu.jo) to meet at any other time.*

REFERENCES AND LEARNING RESOURCES

Required Textbook:

- Yuri Diogenes and Erdal OzkayaCybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition

Suggested Additional Resources:

- Building Secure & Reliable Systems Best Practices for Designing, Implementing and Maintaining Systems by Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea & Adam Stubblefi eld ,16-3-2020
- CYBER SECURITY ESSENTIALS Edited by James Graham Richard Howard Ryan Olson , 2011
- Justin Seitz. Black Hat Python: Python Programming for Hackers and Pentesters. No Starch, 2014.
- Sean-Philip Oriyano, Robert Shimonski. Client-Side Attacks and Defense 1st ed. Syngress, 2012.
- Christopher Hadnagy, Social Engineering: The Art of Human Hacking. Wiley, 2011.
- Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2/E. Wiley, 2011.
- Gordon Fyodor Lyon. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Nmap Project, 2009.
- Jon Erickson. Hacking: The Art of Exploitation 2/E. No Starch Press, 2008.

Useful Web Resources:

Open Security Training, http://www.opensecuritytraining.info,
Corelan Team, http://www.corelan.be,

COURSE OBJECTIVES

The course is designed to help students gain a detailed insight into the practical and theoretical aspects of advanced topics in defense cyber and intrusion detection. It aims to:

- Understand the approaches used today by computer attackers.
- Understand the offensive and defensive techniques of computer attacks.
- Gain solid knowledge in memory corruption concepts and the ability to exploit, and defend against them.
- Demonstrate the value of Web App attacks such as: SQL injection, Cross-Site Scripting, and Web Session attacks.
- Know and apply advanced technologies related to cyber defense such as Snort IDS/IPS etc .
- Demonstrate basic abilities to analyze malware.
- Provide hands-on labs addressing scanning, exploiting, and defending systems.

ACADEMIC SUPPORT

It is The Hashemite University policy to provide educational opportunities that ensure fair, appropriate and reasonable accommodation to students who have disabilities that may affect their ability to participate in course activities or meet course requirements. Students with disabilities are encouraged to contact their Instructor to ensure that their individual needs are met. The University through its Special Need section will exert all efforts to accommodate for individual's needs.

Special Needs Section:

Tel: 053903333 EXT 5023/4583

Location: (https://hu.edu.jo/facnew/index.aspx?typ=68&unitid=70000000)

Email: (huniv@hu.edu.jo)

COURSE REGULATIONS

Participation

Class participation and attendance are important elements of every student's learning experience at The Hashemite University, and the student is expected to attend all classes. A student should not miss more than 15% of the classes during a semester. *Those exceeding this limit of 15% will receive a failing grade regardless of their performance*. It is a student's responsibility to monitor the frequency of their own absences. **Attendance record begins on the first day of class irrespective of the period allotted to drop/add and late registration. It is a student's responsibility to sign-in; failure to do so will result in a non-attendance being recorded.**

In exceptional cases, the student, with the instructor's prior permission, could be exempted from attending a class provided that the number of such occasions does not exceed the limit allowed by the University. The instructor will determine the acceptability of an absence for being absent.

A student who misses more than 25% of classes and has a valid excuse for being absent will be allowed to withdraw from the course.

Plagiarism

Plagiarism is considered a serious academic offence and can result in your work losing marks or being failed. HU expects its students to adopt and abide by the highest standards of conduct in their interaction with their professors, peers, and the wider University community. As such, a student is expected not to engage in behaviours that compromise his/her own integrity as well as that of the Hashemite University.

Plagiarism includes the following examples and it applies to all student assignments or submitted work:

- **Use of the work, ideas, images or words of someone else without his/her permission or reference to them.**
- **Use of someone else's wording, name, phrase, sentence, paragraph or essay without using quotation marks.**
- **Misrepresentation of the sources that were used.**

The instructor has the right to fail the coursework or deduct marks where plagiarism is detected

Late or Missed Assignments

In all cases of assessment, students who fails to attend an exam, class project or deliver a presentation on the scheduled date without prior permission, and/or are unable to provide a medical note, will automatically receive a fail grade for this part of the assessment.

- Submitting a term paper on time is a key part of the assessment process. Students who fail to submit their work by the deadline specified will automatically receive a 10% penalty. Assignments handed in more than 24 hours late will receive a further 10% penalty. Each subsequent 24 hours will result in a further 10% penalty.
- In cases where a student misses an assessment on account of a medical reason or with prior permission; in line with University regulations an incomplete grade for the specific assessment will be awarded and an alternative assessment or extension can be arranged.

Student Complaints Policy

Students at Hashemite University have the right to pursue complaints related to faculty, staff, and other students. The nature of the complaints may be either academic or non-academic. For more information about the policy and processes related to this policy, you may refer to the students' handbook.

COURSE ASSESSMENT

Course Calendar and Assessment

Students will be graded through the following means of assessment and their final grade will be calculated from the forms of assessment as listed below with their grade weighting taken into account.

Assessment	Grade Weighting	Deadline Assessment
Midterm exam	30%	To be announced
Project	20%	To be announced
Presentations and Assignments	10%	Monthly
Final Exam	40%	To be announced

Description of Exams:

Test questions will predominately come from the material presented in the lectures. Semester exams will be conducted during the regularly scheduled lecture period. Exam will consist of a combination of multiple-choice, short answer, match, true and false and/or descriptive questions.

Homework:
Will be given for each chapter, while the chapter in progress you are supposed to work on them continuously and submit in next lecture when I finish the chapter.
You are also expected to work on in-chapter examples, self-tests and representative number of end of chapter problems. The answers of self-tests and end of chapter exercises are given at the end of the book.

Quizzes: Unannounced quizzes will be given during or/and at the end of each chapter based upon the previous lectures. It will enforce that you come prepared to the class.
No make-up exams, homework, or quizzes will be given. Only documented absences will be considered as per HU guidelines.

Grades are not negotiable and are awarded according to the following criteria*:

Letter Grade	Description	Grade Points
A+	Excellent	4.00
A		3.75
A–		3.50
B+	Very Good	3.25
B		3.00
B–		2.75
C+	Good	2.50
C	Fail	2.25

WEEKLY LECTURE SCHEDULE AND CONTENT DISTRIBUTION

Course Plan

Week no.	Topic	chapters
1+2	**Introduction:** • Introduction to cyber security • Information Assurance Fundamentals • Cyber Security Fundamentals • Quality of an IS • DoS attack • The Domain Name System (DNS) • Security and the DNS	
3+4	Exploitation • Techniques to Gain a Foothold	

Week no.	Topic	chapters
	• Integer Overflow Vulnerabilities • Stack-Based Buffer Overflows • Protecting against Stack-Based Buffer Overflows • Addendum: Stack-Based Buffer Overflow Mitigation • Format String Vulnerabilities • SQL Injection • Protecting against SQL Injection	
5+6	UNIX rsyslog package • Multi-threading • TCP, SSL, TLS, RELP • MySQL, PostgreSQL, Oracle and more • Filter any part of syslog message • Fully configurable output format • Suitable for enterprise-class relay chains	
7	Malicious Codes • Self-Replicating Malicious Code • Viruses • Worms • Evading Detection and Elevating Privileges • Obfuscation • Virtual Machine Obfuscation • Persistent Software Techniques • Rootkits	
8	Defense and Analysis Techniques • Memory Forensics • Honeypots • Malicious Code Naming • Passive Analysis • Active Analysis	
9	Mitigating Denial–of–Service Attacks	

Week no.	Topic	chapters
	• Types of attack mitigations • Traffic scrubbing • Source or location blocking • Pattern and behaviour blocking • Disabling dynamic functions • Displaying CAPTCHA	
10	Disaster Planning • cybersecurity disaster recovery plan • Data protection. • Loss minimization • Restoration • Establish a monitoring plan.	
11	Simple Event Correlator Crisis Management • Overview of SEC • Security Event Processing with Simple Event Correlator • Monitoring SSH login failures and blocking suspicious hosts • Cross-correlating offending events from Netfilter, SSH, and Apache logs	
12	network intrusion detection • Intrusion detection category • Detection method • Anomaly-based • Classification	
13	Snort IDS/IPS	

Week no.	Topic	chapters
	• Features of SNORT • Packet Logging • Analysis of Protocol • Sniffer Mode • Packet Logger Mode • Network Intrusion Detection System Mode	
14	iDefense Special File Investigation Tools • TOOL DEVELOPMENT Visual Studio C++ Express • Swftools • Malzilla • Dezend • Process Hacker • mmunity debugger	
15	**Student Presentations**	