CYBER SECURITY BASICS

A Hands-on Approach

LENGTH:	6 weeks
EFFORT:	5 - 7 hours per week
SUBJECT:	Computer Science
LEVEL:	Intermediate
LANGUAGE:	English
VIDEO TRANSCRIPTS:	English

SYLLABUS

INTRODUCTION

Cyber Security Basics: A Hands-on Approach presents a practical cybersecurity overview composed of 6 lectures. Theoretical explanations, essential for an appropriate comprehension of all concepts, are supported by examples and tools to guarantee a comprehensive learning process. After an introduction to cybersecurity to contextualize its relevance and significance, the main well-known techniques, concepts and tools for a cybersecurity beginner are presented.

A wide range of videos is provided to enhance the students' learning experience, together with different activities like forums, homework or self-assignments, to motivate and guide students. The course follows a hands-on approach, thus promoting the knowledge acquisition by personal, first-hand practical working scenarios.

In order to attract the attention of a wide community, this course is introductory in nature and will be taught in English.

If this is your first course on edX, do not hesitate to enroll in the Demo course to get to know the courseware: https://www.edx.org/course/demox-edx-demox-1.

OBJECTIVES

After finishing the course students will have achieved the following goals:

- Basic knowledge and skills of reverse engineering.
- Understand computer forensic processes and some managed traces.
- Skills to proactively and reactively manage and monitor common cybersecurity attacks.
- Understand how malware works, how can it become persistent and how it can be detected.
- Skills to identify and manage common vulnerabilities.
- Basic knowledge and skills of penetration testing.

COURSE STAFF

- Lorena González Manzano is lecturer at Universidad Carlos III de Madrid.
- José María de Fuentes García-Romero de Tejada is lecturer at Universidad Carlos III de Madrid.
- Pedro Peris López is associate professor at Universidad Carlos III de Madrid.
- Juan M. Estévez Tapiador is associate professor at Universidad Carlos III de Madrid.
- José René Fuentes Cortez, is assistant professor at Universidad Carlos III de Madrid.

The participation of each member is scheduled as follows considering that S = Supervision, CC= Content Creation, SG = Student guidance and CM=community manager:

Lectures	Lorena González	José María de Fuentes	José René Fuentes	Pedro Peris	Juan M. Estévez
1	S, CM				CC, SG
2	S, CC, CM				
3	S, CM	SG	CC		
4	S	CM		CC, SG	
5	S	CC, SG, CM			
6	S, CC, SG	CM			

COURSE STRUCTURE

Lecture 1. Cybersecurity: an overview
This lecture introduces the impact of cybersecurity nowadays, as well as some examples of cyberthreats that motivate the relevance of this area of study. In particular, the emergence of cybersecurity from the beginning of the internet development is firstly introduced. Types of cyberthreats, such as cybercrime or cyberwarfare, are later described, together with an overview of the current cyberthreat landscape. Finally, some well-known cybersecurity events are presented, like Ashley Madison database attack or hacked Chrysler cars.
Lecture structure:
Cybersecurity landscape and history
Cyberthreats: definition and types
Well-known recent cybersecurity events.
Lecture 2. Computer forensics
This lecture introduces computer forensics, that is the technique focused on the analysis and preservation of evidences in a particular computer device after an attack occurs. Secondly, common forensic traces are defined. In particular, studied traces refer to deleted files and hidden data. Additionally, tools to deal with these traces are also introduced. Finally, Autopsy, a tool to manage forensic cases as a whole, is presented.
Lecture structure:
Basic concepts of computer forensics

Common forensic traces.
Description of forensic report writing.
Practical case.
Lecture 3. Assembly programming: towards reversing
This lecture introduces the main concepts of reverse engineering, that is, the ability to take an executable element and try to figure out how it works. Firstly, the definition of this technique is described, as well as the relevance of its use. Secondly, the description of computer memory and the explanation of computer instructions are described, which are considered the main basic concepts of reversing. Thirdly, the distinction between decompiling and disassembling is introduced. After some theoretical knowledge, examples of decompiling codes in different languages, namely Java and C, are presented. The required tools for this action will be easily presented. Similarly, some disassembly examples are also described together with the introduction of a common assembler tool, IDAPro. Given the difficulty of disassembly, there are various examples to show assorted assembly features.
Lecture structure:
Definition of reverse engineering and the necessity of assembly programming.
Computer memory description.
Decompiling and disassembling.
Disassembling in a x86 architecture.
Lecture 4. Cyberdefense
This lecture presents the main concepts of cyberdefense. After an introduction to this topic, firewalls are outlined. Their definition and their main uses are explained to later introduce one of the most common firewalls tools for Linux, IPTABLES. Main features of this tool and examples to illustrate its use are described. The following part involves the description of Intrusion Detection Systems (IDSs), being focused on SNORT tool. Likewise, examples are proposed to show the essential features of SNORT. Finally, Security Information and Event management (SIEM) systems, which refer to a general approach to manage cyberdefense, are presented.
Lecture structure:
Definition and introduction to cyberdefense.
Definition and introduction to firewalls.
Definition and introduction to Intrusion Detection Systems (IDSs).
Definition and introduction to Security Information and Event management (SIEM) systems.

Lecture 5. Malware and Advanced Persistent Threats (APTs)
This lecture explains the main concepts related to malware and Advanced Persistent Threats (APTs), together with the main techniques to achieve their identification. Firstly, the definition and types of malware are presented. Secondly, tools to perform malware analysis are described. Finally, APTs are introduced and some APTs real cases are outlined.
Lecture structure:
Definition of malware and types.
Definition of Advanced Persistent Threats (APTs).
Lecture 6. Vulnerabilities and exposures
This last lesson presents vulnerabilities description and management. It presents the description and examples of the most common vulnerabilities at software, network and web level. Specifically, at software level, segmentation faults, race conditions and input validation vulnerabilities are described; at network level, password sniffing, session hijacking and denial of service attacks are introduced; and at web level, Cross Site Scripting (XSS), SQL Injection and the disclosure of too much information vulnerabilities are described. After the introduction of common vulnerabilities, the definition, use and application of penetration testing (pentesting) are explained. Besides, Metasploit, one of the most well-known tools to perform pentesting, is introduced. Finally, the necessity of vulnerability repositories and the presentation of the most common one, Common Vulnerabilities and Exposures (CVE) developed by MITRE corporation, are presented.
Lecture structure:
Definition of common vulnerabilities and exposures.
Introduction to common software vulnerabilities.
Introduction to common network vulnerabilities.
Introduction to common web vulnerabilities.
Pentesting with Metasploit.
Presentation of vulnerability repositories: Common Vulnerabilities and Exposures (CVE).

COURSE METHODOLOGY

Each lecture is composed of a set of videos that describe all proposed topics. Some videos describe theoretical content and some others present examples of applied tools and techniques. Moreover, given the hands-on focus of this course, all topics are reinforced with practical assignments with growing hardness. For these assignments, applied tools are open source and the installation of all required software will be appropriately guided. It guarantees the successfulness of the learning process achieving that all established exercises are properly completed.

Multiple supportive materials are also included in each lecture to guide students in the learning process. In sum, the following teaching items are noticed:

- **Videos** explain all theoretical and practical content students have to learn in each different lecture.
- **Additional readings** refer to material provided by teachers, namely articles, news, etc. which are convenient to identify the relationship between theoretical contents and what is happening in the world. Moreover, after readings, some graded questions are presented.
- **Homeworks** refer to exercises that students have to do on their own to complete knowledge of a specific topic. Answers will be provided, being some of them presented in the form of videos. However, we do not recommend accessing to solutions until having done each homework.
- **Knowledge check** is equivalent to an exam, that is, a set of questions to check the knowledge of some content of the course.
- **Additional materials**, such as application manuals, guides, links to useful websites, etc.

The estimated time learners need to complete each week is from 5 to 7 hours.

COMMUNICATION WITH LEARNERS

The **COURSE INFO PAGE** will be used to keep the students up to date in all the relevant aspects of the course.

Learners community **FORUM** will be used to encourage engagement and interaction with students.

Weekly **EMAILS** will be used to keep students up-to-date with the course development.

Follow us on **TWITTER** with the hashtag #CyberSecurityedX

EVALUATION

There are 8 **EXAMS**:

- 1 final exam: at the end of the course there is a final assessment that is graded the **20%** of the total grade.
- 7 partial exams: one per week except for week 1, where 2 assessments are included. The total weight of these 7 exams is **60%** of the total grade of the course.

Besides, there are 10 **READINGS** that are followed by some graded questions. The readings are graded the **20%** of the total grade.

The summary of exams and readings in each lecture is presented in the following table:

WEEK	CONTENTS	Marks of exams	Marks of readings
1	*Lecture 1. Cybersecurity: an overview* Test (graded)	**5%**	
	Lecture 2. Computer forensics Reading (graded) Test (graded)	**5%**	**2%**
2	*Lecture 3. Assembly programming: towards reversing* Reading (graded) Test (graded)	**10%**	**2%**
3	*Lecture 4. Cyberdefense* 3 Readings (graded) Test (graded)	**10%**	**6%** (3 x 2%)
4	*Lecture 5. Malware and Advanced Persistent Threats (APTs)* 2 Readings (graded) Test (graded)	**10%**	**4%** (2 x 2%)
5	*Lecture 6. Vulnerabilities and exposures (part 1)* 2 Readings (graded) Test (graded)	**10%**	**4%** (2 x 2%)
6	*Lecture 6. Vulnerabilities and exposures (part 2)* Reading (graded) Test (graded)	**10%**	**2%**
6	Final Exam	**20%**	

Passing the course requires obtaining 60% of the final grade.

This course also includes non graded activities: a variety of self-assessments (called knowledge checks) and homeworks. Though these activities are not part of the assessment process, they contribute to the learning experience.

CALENDAR

The course ***Cyber Security Basics: A Hands-on Approach*** starts on 10 April and will be available until 30 June (23:59 UTC) as a self-paced course. The time of the course is always UTC (Coordinated Universal Time).

Certificates will be available on demand for learners as soon as they complete enough of the course with a high enough grade to qualify for a certificate.