Course guides
230994 - MALW - Malware

Last modified: 16/06/2020

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 701 - DAC - Department of Computer Architecture.

Degree: MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Compulsory subject).

Academic year: 2020 **ECTS Credits:** 5.0 **Languages:** Catalan, English, Spanish

LECTURER

Coordinating lecturer: René Serral Gracià

Others:

PRIOR SKILLS

The student must have previous knowledge of programming in Python, C, C++ and x86 assembler, code development, debugging and capacity of developing complex programs written in C++.
The student must have previous knowledge about operating systems and application development using the generic system call interface.

REQUIREMENTS

None

TEACHING METHODOLOGY

Theory, Laboratory, Cooperative work, Short exams, Advisement

LEARNING OBJECTIVES OF THE SUBJECT

1.- Know the concept of process and the operating system management structures.
2.- Know how to construct the logical address space of a process in a modern operating system together with the management structures to store that information.
3.- Know the differences between user mode and kernel mode.
4.- Know multithreading programming together with the per-thread management structures.
5.- Know the philosophy behind a Windows and Linux operating systems
6.- Know and differentiate the different malware categories
7.- Know every phase of a malware: intrusion, infection, obfuscation and payload
8.- Know the different alternatives to deploy a malware code in an operating system
9.- Know the different implementation of the infection phase of a malware code
10.- Know the different alternatives to obfuscate and hide malware
11.- Develop a malware able to infect and hide a Windows operating system
12.- Know the basic components of an antivirus software and how they work in a 32 and 64 bits Windows operating system
13.- Discuss the ethical implications of creating and propagating malware

STUDY LOAD

Type	Hours	Percentage
Self study	86,0	68.80
Hours large group	26,0	20.80
Hours small group	13,0	10.40

Total learning time: 125 h

CONTENTS

Operating system concepts

Description:
This chapter describes the concept of process together with the operating system management structures: PCB, page table (address translation), process sections and operating system calls in Windows.

Full-or-part-time: 4h
Theory classes: 4h

Malware categorization

Description:
This chapter describes the concept of malicious code and its different phases. The different malware categories will be presented highlighting the global and per-phase differences.

Full-or-part-time: 10h
Theory classes: 2h
Laboratory classes: 2h
Self study : 6h

Techniques of infection propagation

Description:
This chapter describes the current techniques of infection propagation: social engineering, exploits, buffer overflow, stack overflow… Techniques to store the malware in an infected machine will be discussed.

Full-or-part-time: 36h
Theory classes: 4h
Laboratory classes: 8h
Self study : 24h

Obfuscation and malware stealth techniques

Description:
This chapter describes several techniques to prevent malware from being detected together with the mechanism to implement them: code injection, process hollowing and API redirection.

Full-or-part-time: 38h
Theory classes: 8h
Laboratory classes: 6h
Self study : 24h

Antivirus

Description:
This chapter describes the different components of an antivirus software and how they interact with the operating system. Malware counterattacks will be also discussed.

Full-or-part-time: 29h
Theory classes: 2h
Laboratory classes: 2h
Self study : 25h

Ethics about malware utilization

Description:
This chapter will describe the ethical side of malware

Full-or-part-time: 2h
Theory classes: 2h

Final examination

Description:
Final Examination

Full-or-part-time: 18h
Guided activities: 2h
Self study : 16h

GRADING SYSTEM

The evaluation of the course is composed by three major components:
- Final exam about the theory of the course
- Project consisting in the implementation of several components of malware
- Presentations of other techniques implemented in malware

The final grade is composed by:
Final grade = 30% final exam + 40% project + 30% presentations

BIBLIOGRAPHY

Basic:
- Skoudis, E.; Zeltser, L. Malware: fighting malicious code. Upper Saddle River, NJ: Prentice Hall PTR, 2004. ISBN 0131014056.
- Ligh, M.H.; Case, A.; Levy, J.; Walters, A. The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac Memory [on line]. Indianapolis, IN: John Wiley & Sons, 2014 [Consultation: 15/07/2020]. Available on: https://ebookcentral.proquest.com/lib/upcatalunya-ebooks/detail.action?docID=1740753. ISBN 9781118825044.

Complementary:
- Silberschatz, Abraham; Galvin, Peter B; Gagne, Greg. Operating system concepts. 9th ed., international student version. Hoboken: John Wiley & Sons, cop. 2014. ISBN 9781118093757.
- Yosifovich, Pavel; Ionescu, Alex; Russinovich, Mark E; Solomon, David A. Windows internals : part 1: system architecture, processes, threads, memory management, and more. Seventh edition. Redmond, Washington: Microsoft Press, [2017]. ISBN 9780735684188.