

# **REVERSE ENGINEERING – CLASS 0x00**

## **ADMINISTRATIVE INFORMATION**

Cristian Rusu

# **TABLE OF CONTENTS**

- **who we are**
- **organization**
- **evaluation**
- **structure of the course**
- **objectives**
- **general references**

# WHO WE ARE

- **Cristian Rusu**
  - course
  - contact: [cristian.rusu@unibuc.ro](mailto:cristian.rusu@unibuc.ro)
  - class web page: <https://cs.unibuc.ro/~crusu/re/index.html>
  
- **Cristian-Cătălin Nicolae and Alexandru Mocanu**
  - lab work
  - contact
    - [cristian-catalin.nicolae@unibuc.ro](mailto:cristian-catalin.nicolae@unibuc.ro)
    - [alexandru.mocanu@s.unibuc.ro](mailto:alexandru.mocanu@s.unibuc.ro)

# ORGANIZATION AND EVALUATION

- **organization:**
  - 1h course / week
  - 2h lab work / 1 week
- **evaluation:**
  - 60% lab work during the semester
  - 40% final project (multiple RE tasks)
- **how to pass:**
  - > 50% for the lab work
    - you can miss (unannounced) a maximum of two lab session
    - lab sessions are mandatory to pass in the same year
  - > 50% final project
  - **both are hard limits!**

# ORGANIZATION AND EVALUATION

- **for the course**
  - we talk about the big ideas in RE
  - concept/methods/techniques
  - here, the ideas are important
- **for the lab work: you will need a laptop to be able to run all the lab work during the semester**
  - practice, practice, practice
  - a lot of programming
  - Assembly x86
  - basic Windows/Linux/Git/python/C/OS knowledge is assumed

# ORGANIZATION AND EVALUATION

- the expected work-load

## 2. Date despre disciplină

2.1. Denumirea disciplinei		Inginerie inversă și tehnici de securizare a codului						
2.2. Titularul activităților de curs				Lector dr. Ruxandra-Florentina Olimid				
2.3. Titularul activităților de seminar / laborator / proiect				Lector dr. Ruxandra-Florentina Olimid				
2.4. Anul de studiu	II	2.5. Semestrul	II	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Conținut <sup>1)</sup>	DS
							Obligativitate <sup>2)</sup>	DI

## 3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	3	din care: 3.2. curs	1	3.3. seminar/ laborator/ proiect	2
3.4. Total ore pe semestru	30	din care: 3.5. curs	10	3.6. SF	20
<b>Distribuția fondului de timp</b>					<b>Ore</b>
3.4.1. Studiul după manual, suport de curs, bibliografie și notițe – nr. ore SI					56
3.4.2. Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
3.4.3. Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					70
3.4.4. Examinări					4
3.4.5. Alte activități					
3.7. Total ore studiu individual	150				
3.8. Total ore pe semestru	180				
3.9. Numărul de credite	6				

# **NO PLAGIARISM IS ALLOWED**

- **you will fail the class**
- **you will be reported to the appropriate institutional offices**
- **NO copy/paste anywhere**
- **do not copy from your colleagues (responsibility is shared)**

# STRUCTURE OF THE COURSE

- **Introduction to RE**
- **x86 crash course**
- **Static analysis**
- **Dynamic analysis**
  
- **Smashing the stack**
- **NX/DEP, ASLR, ROP**
  
- **RE for other platforms (not Win32 and Linux)**
- **Further topics**



# OBJECTIVES

- **understand what an executable does and how it works**
- **go from binaries back to something resembling source code**
- **pitfall due to architecture and coding issues**
- **exploit binaries**

# OBJECTIVES

- **you will be able to analyze a binary executable**
  - understand CPU execution
  - analyze CPU instructions
  - follow execution paths and logic
  - monitor the interactions with the OS and other software
  - in many ways, you will become a detective of some sort

# OBJECTIVES

- **Jobs in:**
  - cybersecurity
  - malware analysis
  - gaming
  - academia/research
  - ...
  - in general, RE boosts your profile

# GENERAL REFERENCES

- Radu Caragea, Binary Reverse Engineering And Analysis (2021), [https://pwnthybytes.ro/unibuc\\_re](https://pwnthybytes.ro/unibuc_re)
- Alex Gantman, In Defense of Reverse Engineering, <https://againsthimself.medium.com/in-defense-of-reverse-engineering-e07fe19b26c>
- Eldad Eilam, Reversing: Secrets of Reverse Engineering
- Jon Erickson, Hacking: The Art of Exploitation
- Bruce Dang et. al., Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

