Practical Network Defense

Master's degree in Cybersecurity 2020-21

Course introduction

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

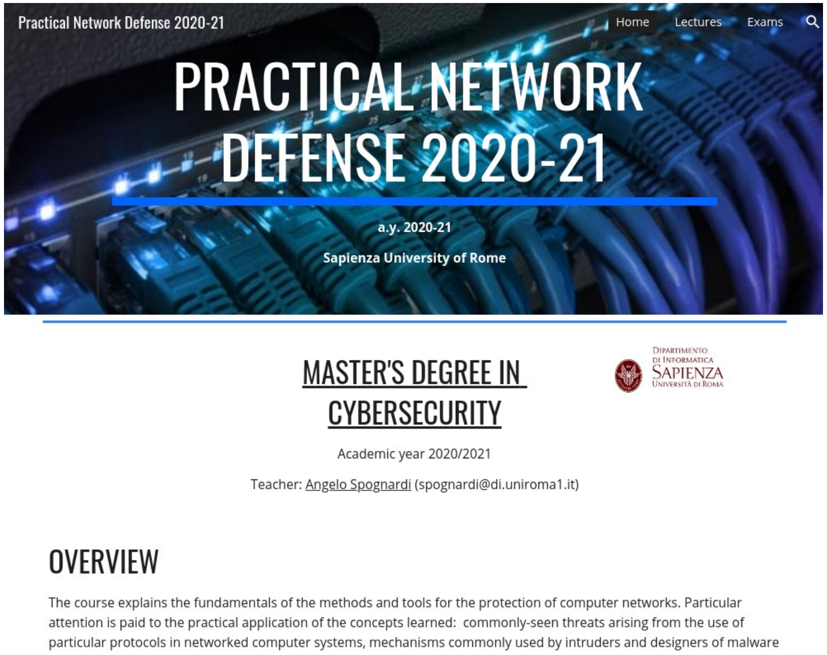
Practical Info

The lecturer

- Angelo Spognardi
  - Associate professor, Dipartimento di Informatica
  - Tel: 06 4925 5164
  - https://angelospognardi.site.uniroma1.it
  - spognardi@di.uniroma1.it
- Student hours:
  - Until COVID emergency: on request by email
  - After: my office G28, v.le Regina Elena, 295, Edificio G
- My research interests:
  - Computer network security, security in social networks, privacy, applied cryptography, operating systems, programming

This course

- Website: https://sites.google.com/di.uniroma1.it/netdef2021
  - Join the class in classroom classroom.google.com using this code: jav362c
  - Use your @studenti.uniroma1.it account (or it won’t work…)
- 6 CFUs
- Schedule:
  - Monday 17-19 Aula Alfa
  - Thursday 12-15 Tiburtina Labs (lab XV)


Practical Network Defense 2020-21
Home
Lectures
Exams

PRACTICAL NETWORK DEFENSE 2020-21

a.y. 2020-21

Sapienza University of Rome

MASTER'S DEGREE IN CYBERSECURITY

Dipartimento di Informatica
Sapienza
Università di Roma

Academic year 2020/2021

Teacher: Angelo Spognardi (spognardi@di.uniroma1.it)

OVERVIEW

The course explains the fundamentals of the methods and tools for the protection of computer networks. Particular attention is paid to the practical application of the concepts learned: commonly-seen threats arising from the use of particular protocols in networked computer systems, mechanisms commonly used by intruders and designers of malware

Objectives

- Methods and tools for the protection of computer networks
- Focus on practical application of the concepts learned:
  - protocols in networked computer systems
  - mechanisms commonly used to compromise a computer system's security
  - mechanisms used for the detection of intrusion attempts in computer networks
- At the end of the course students will be able to:
  - monitor traffic in networks
  - apply a security policy
  - perform a network scan and search for vulnerabilities in a computer network
- Students will develop the ability to:
  - select the appropriate firewall rules to protect a network
  - select the most appropriate mechanisms to protect a networked computer system
  - make the most appropriate design choices to implement a "defense in depth" strategy, using isolated networks and dedicated tools (VPN, proxy and firewall)
- Students will learn how to document their choices, also through the use of automated reporting tools. They will also have acquired the ability to prepare presentations related to specific scientific topics

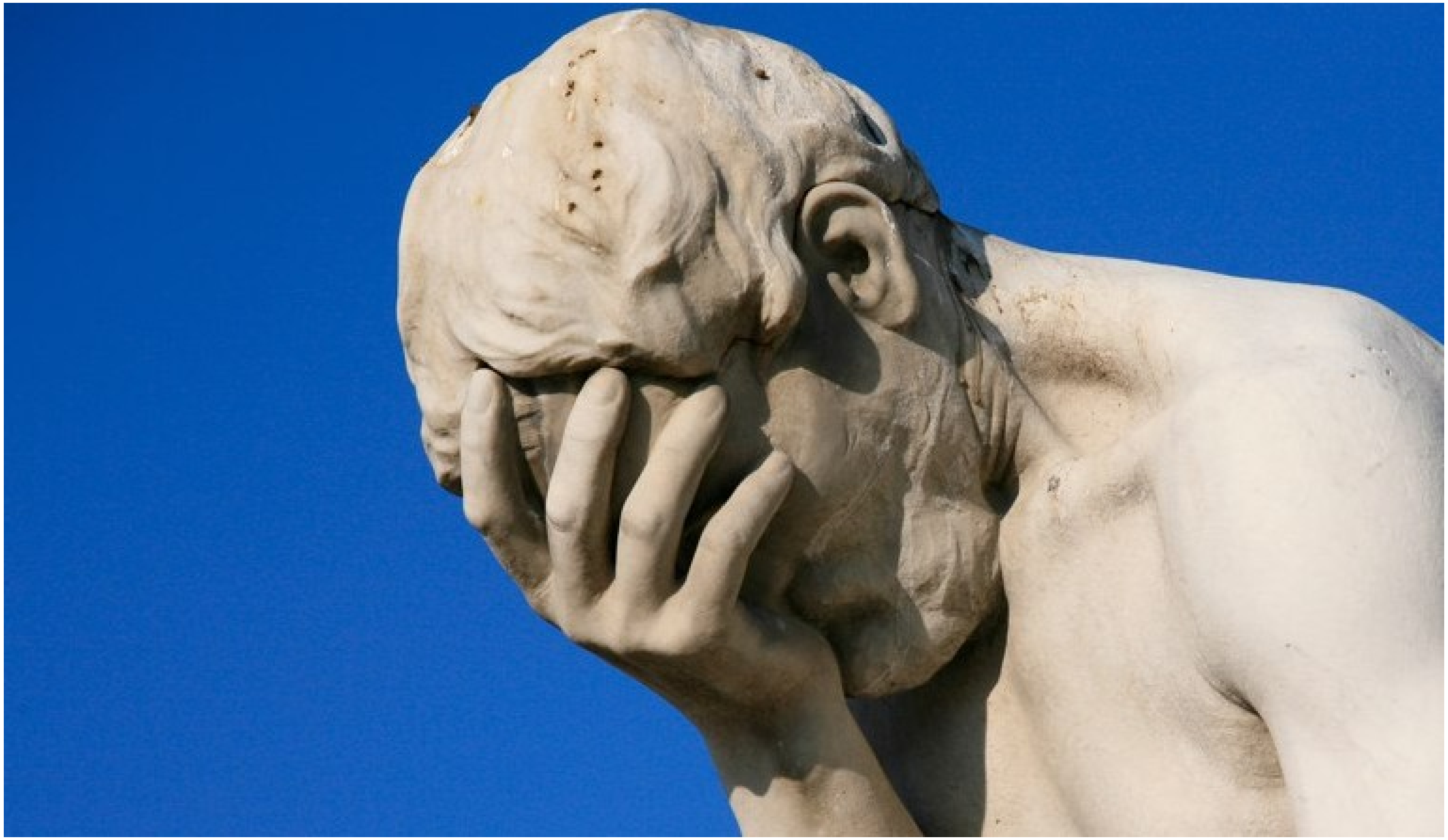
Topics covered (tentative)

- Network monitoring
- Network traffic analysisNetwork attacks (e.g., session hijacking, man-in-the-middle)
- Minimizing exposure (attack surface and vectors)
- Network hardening
- Network policy development and enforcement
- Defense in depth
- Perimeter networks (DMZs)/Proxy Servers
- Implementing firewalls and virtual private networks (VPNs)
- Implementing IDS/IPS
- Network access control (internal and external)

How the classes are structured

- Theoretical concepts presented mainly during classroom hours, but also during lab sessions
- Practical activity during lab hours
- Some topics will have an assignment with two parts:
  1) An implementing part in the virtual lab environment
  2) A reporting part
- Assignments are part of the exam
  - They are a pre-requisite for accessing the written exam

Remember that… things can go bad!!



Especially during labs… Please be tolerant with us ☺

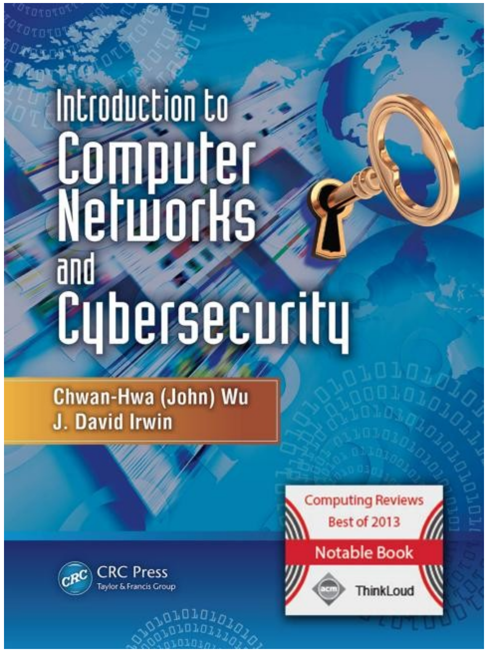
To do the first activities

- We will use Kathará (formerly known as netkit)
  - A container-based framework for experimenting computer networking: http://www.kathara.org/
- A virtual machine is made ready for you: please download it **BEFORE** coming to the labs
  - https://drive.google.com/file/d/1W6JQzWVyH5_LKLD20R6XH1ugPDP5LWP5/view?usp=sharing
- After you will be granted the access to our virtual infrastructure (the ACME co.)

How to pass the exam

- All the rules are applied both to full-time and part-time students
  - 4 mandatory assignments
  - full written exam
  - (optional) on demand oral exam for students with a written exam >= 27
- Assignment rules
  - Assignments are individual or group activities to apply techniques and tools introduced during the classes
  - Assignments do not have an hand-in date, but must be handed-in before taking the full-exam
  - Assignments are evaluated A, B or C and provide an increment to the final grade of the written exam (up to +3 points)
- Written exam rules
  - A written exam is valid for one year and supersedes any other written exam done previously

Material

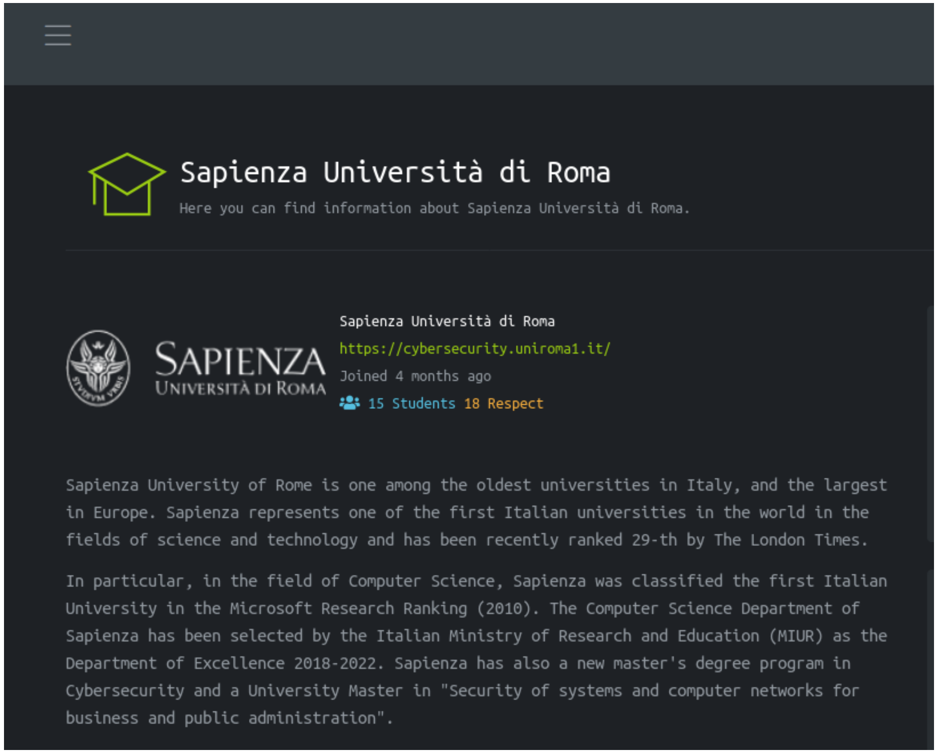


- Hand-notes
- Slides of the lectures
- Articles linked in the website
- Main textbook:
  - **Introduction to Computer Networks and Cybersecurity** (Chwan-Hwa (John) Wu, J. David Irwin, 1e) CRC Press
- Other books will be suggested during the lectures for each considered subject
  - Your contribution is welcome: don’t hesitate to share useful resources via classroom

Feedback

- Always welcome
- Write me your suggestions

Hack the box!



Sapienza Università di Roma

Here you can find information about Sapienza Università di Roma.

Sapienza Università di Roma
https://cybersecurity.uniroma1.it/
Joined 4 months ago
15 Students 18 Respect

Sapienza University of Rome is one among the oldest universities in Italy, and the largest in Europe. Sapienza represents one of the first Italian universities in the world in the fields of science and technology and has been recently ranked 29-th by The London Times.

In particular, in the field of Computer Science, Sapienza was classified the first Italian University in the Microsoft Research Ranking (2010). The Computer Science Department of Sapienza has been selected by the Italian Ministry of Research and Education (MIUR) as the Department of Excellence 2018-2022. Sapienza has also a new master's degree program in Cybersecurity and a University Master in "Security of systems and computer networks for business and public administration".

https://www.hackthebox.eu/

- Website with CTF (capture the flag) challenges
- Join our team (and please do your job!)
- To be enrolled:
  - Register yourself in the website
  - Join our telegram group https://t.me/htbsapienza
  - Write in the group your hack-the-box username

Self-assessment!

What is this assessment about?

- If you can not understand some questions at all, you are **definitely lacking** the necessary prerequisites
- If you understand the questions, but just cannot remember the answers, you may think you would look in the book (or would google)…
- You can find the answers in most elementary books on computer security and using your computer (as a engineer would)
- But do not cheat yourself – we will be using the commands and the terms asked about in the test all through the course…
  - Don't get discouraged: simply you have to **fill the gap** to catch up!

Self assessment 1: linux

Self assessment 2: linux2

Self assessment 3: network

Self assessment 4: network2

Self assessment 5: cryptography

That’s all for today

- **Questions?**
- See you next lecture!
- Bonus reference to get used to linux CLI and tools:

  http://overthewire.org/wargames/bandit/bandit0.html

  - Go to bandit and try to reach level 34!!
    - 33 is also good :-)
  - Take notes of the passwords and how you obtained them
  - Try to learn as much as you can solving each level