Practical Network Defense

Master's degree in Cybersecurity 2018-19

Course introduction

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

SAPIENZA
UNIVERSITÀ DI ROMA

Practical Info

The lecturer

- Angelo Spognardi
  - Assistant professor, Dipartimento di Informatica
  - Tel: 06 4925 5164
  - https://angelospognardi.site.uniroma1.it
  - spognardi@di.uniroma1.it
- Student hours:
  - When: Tuesday 10:00-12:00 (please write me in advance)
  - Where: 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/netdef1819/
  - Join the class in classroom classroom.google.com using this code: fsqzvcg
  - Use your @studenti.uniroma1.it account (or it won't work...)
- 6 CFUs
- Schedule:
  - Tuesday 16.30-18.30, Aula1 Castro Laurenziano
  - Thursday 12-14 Tiburtina Labs
  - Friday 09-11 Tiburtina Labs

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

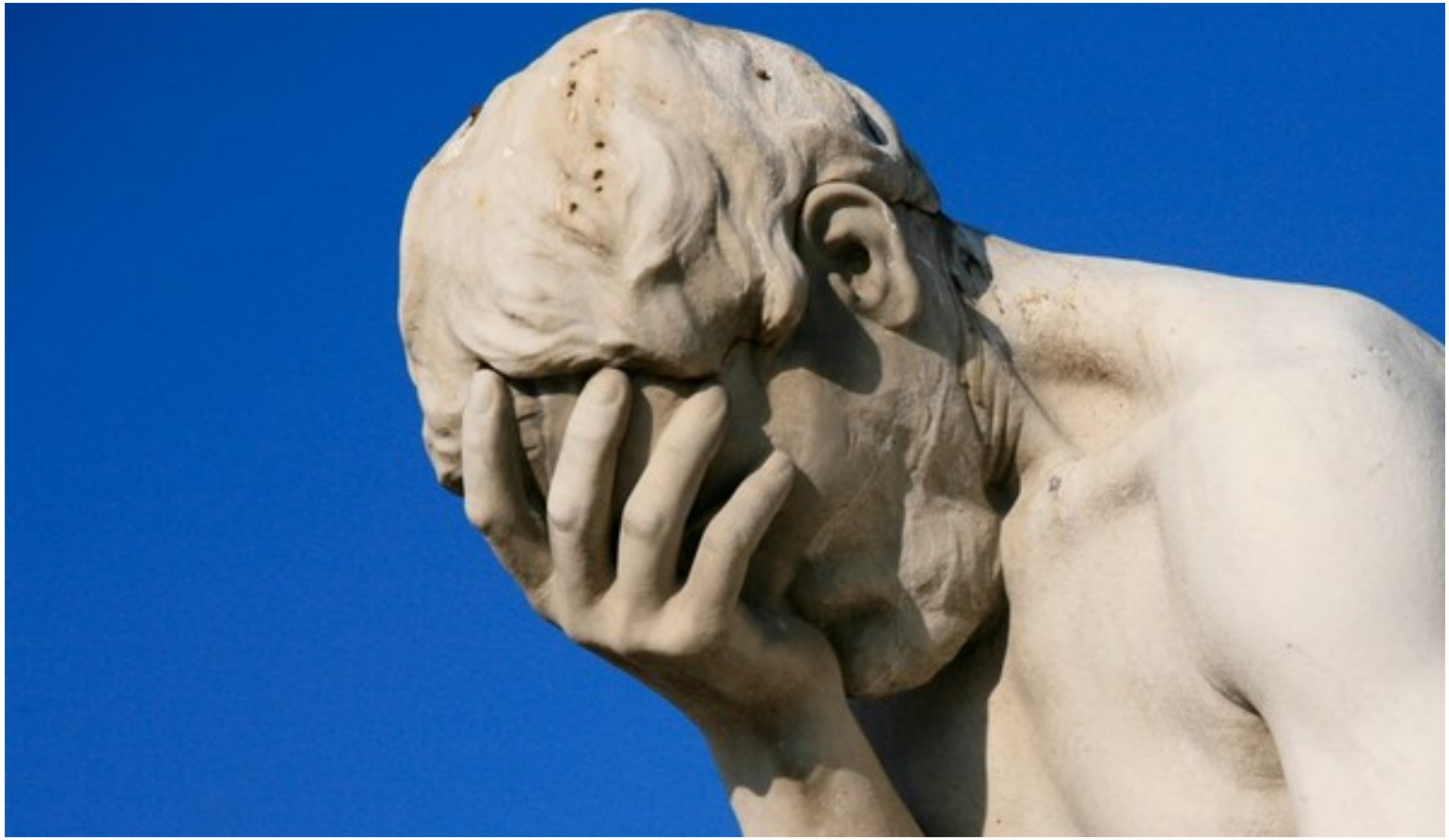
Topics covered (tentative)

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

How the classes are structured

- Theoretical concepts presented mainly during classroom hours, but also during lab sessions
- Practical activity during lab hours
- Each topic will have an assignment with two parts:
  1) An implementing part in the virtual lab environment
  2) A reporting part
- The assignment will undergo a peer-review assessment to improve and fix the implementing part, followed by a in class choral discussion
- At the end the students will have a portfolio with all their reports as a reference

Remember that… things can go bad!!

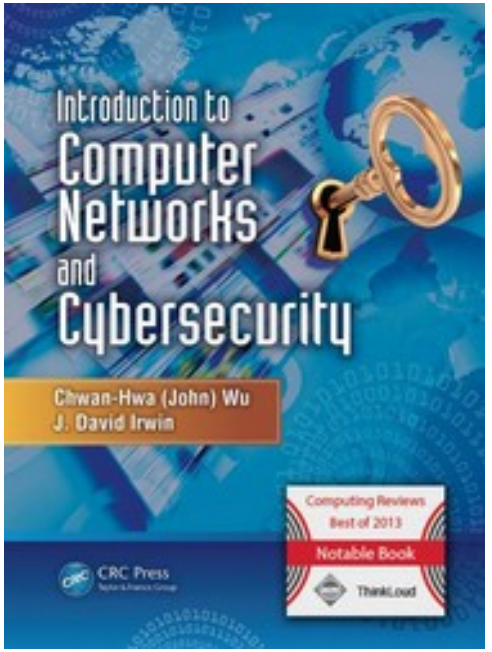


Especially during labs… Please be tolerant with us ☺

How to pass the exam

- Tentative: 2 assessments
  - Mid-term assessment
  - Final term assessment
- Students failing one of them, have to do a full exam
  - if number_of_students > too_many:
    - full_exam=written_exam
  - else:
    - full_exam=oral_exam

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!

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

SAPIENZA
UNIVERSITÀ DI ROMA

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