CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenturesecurity

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

EY Building a better working world

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING

CC.IT warm up

Marina Ribaudo
Università di Genova
marina.ribaudo@unige.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Ethical Hacking
- Capture the Flag
- CyberChallenge.IT Training

The context

- Cyber security has become something nobody can afford to ignore

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

The context

- Many job reports publish data on cyber security skills shortage

[...] there will be 3.5 million unfilled cybersecurity positions by 2021. [...]
Europe faces a projected cybersecurity skills gap of 350,000 workers by 2022

Ethical hacking

- Hacker
  - a computer expert, who tries to understand how systems operate and communicate over a network, how they are designed and how they are protected, whether they are vulnerable, …
- Unfortunately the word **hacker** today has a **negative** connotation

Ethical hacking

LA STAMPA TECNOLOGIA

SEGUICI SU ACCEDI

SEZIONI Cerca...

Huawei e i legami con l'intelligence cinese: la CIA avrebbe le prove | Collettivo di rider pubblica i nomi dei vip che non danno la mancia | Trump perde follower e si lamenta col capo di Twitter | Huawei, via libera al 5G nel Regno Unito | Huawei, il Mate X arriverà a giugno in Cina

Hacker attaccano gli Archivi di Stato: "Più di 5 mila password rubate"

Che si tratti di vandalismo o protesta, le iniziative condotte dai collettivi di pirati informatici dimostrano ancora una volta l'inadeguatezza dei sistemi delle pubbliche amministrazioni

LEGGI ANCHE

Cybersecurity: con "Exodus" un migliaio di italiani spiati per errore dagli hacker di stato

BRUNO RUFFILLI

Ethical hacking

Hackers

White Hat

People who specialized hacking check the faults of the system

Grey Hat

Exploit a security to the attention of the owners

Black Hat

People who break into networks and harm to the network and property

Ethical hacking

White Hat

People who specialized hacking check the faults of the system

We are looking for cyber defender!

Ethical hacking

- CyberChallenge.IT philosophy

hack to learn

NOT learn to hack

Ethical hacking

- Bug Bounty Program
  - allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Bug bounty programs have been implemented by a large number of organizations...
  - https://en.wikipedia.org/wiki/Bug_bounty_program

Ethical hacking

- EU-FOSSA Bug Bounties
  - https://ec.europa.eu/info/news/eu-fossa-bug-bounties-full-force-2019-apr-05_en

```
try {
  var platform = new BugBounty();
  var date = new Date(2019, "Jan", 16*2);
  // TODO: find bugs.
  Participate.toFindBugs().sendToAll();
} catch (NotFoundException ex) {
  std.out("Keep trying", ex);
}
```

Capture the Flag

Capture the Flag

- Cyber security competitions that span over many aspect of computer science, information technology and security education
- Different types
  - Jeopardy
  - Attack/Defense
  - Mixed

https://ctftime.org/

Jeopardy CTF

Competition

- Multiple categories of **challenges**
  - web, binary, crypto, network, misc, ...

Skills

- Jeopardy CTFs allow participants to **think adversariarly**, i.e., to think as an attacker would

Jeopardy CTF

Flag

- Participants must exploit vulnerabilities present into the challenges to find the **hidden flags**

Format

flag{Th1s_is_4_flag_3x@mpl3}

CCIT{this_is_CyberChallenge_flag}

Jeopardy CTF

- Flags are **submitted** to get the **associated scores**
- **Open source software platforms exist** to manage registration of the participants, publication of the challenges, submission of the flags, scoreboard
- We will use CTFd https://ctfd.io/about/

Jeopardy CTF

- The final score is computed by adding up the value of each correctly submitted flag
- Scores can be
  - Static
  - Dynamic

Jeopardy CTF

- The local competion of June will be a Jeopardy CTF

Attack / Defense CTF

Competition

- Teams run an identical machine or network injected with vulnerable services
- Participants must exploit vulnerabilities in opponent' machines while fixing or mitigating flaws in their own

Skills

- Attack/Defense CTFs allow participants to gain experience with both **offensive** and **defensive** related skills

Attack / Defense CTF

Competition

- Usually teams have a couple of hours to understand the playing scenario before the competition starts

Flags

- Are injected in the system at regular intervals called **rounds**
- **Expire** after some rounds

Attack / Defense CTF

- The final score is computed taking into account:
  - The number of flags catched during the competition (**attack** phase)
  - The number of flags lost during the competition (**defense** phase)
  - The amount of time in which the services are available and correctly functioning (**SLA**)

Attack / Defense CTF

- The national competion of July will be an Attack / Defense CTF

Final: July 8-9 2020

- Florence
- Istituto di Scienze Militari Aeronautiche

The National Cyberdefender team

It attends international competitions, such as the European CyberSecurity Challenge (ECSC)

The National Cyberdefender team

Coach

Mario POLINO - PoliMi

Captain

Andrea BIONDO - UniPd

Before ECSC 2019

Two weeks of training in Lucca

Before ECSC 2019: in Rome!

 Rel. 20.02.2020

ECSC 2019: in Bucharest

Bucharest, October 8-11, 2019

ECSC 2019: Silver Medal!

The next three months

CC.IT Training

- We must be realistic...
- You cannot become an expert in three months
  - We will try to give you some foundation on cyber defense on which you can build on during the next three months, and possibly in your professional future
  - We will **have fun** and **grow up together**

CC.IT Training

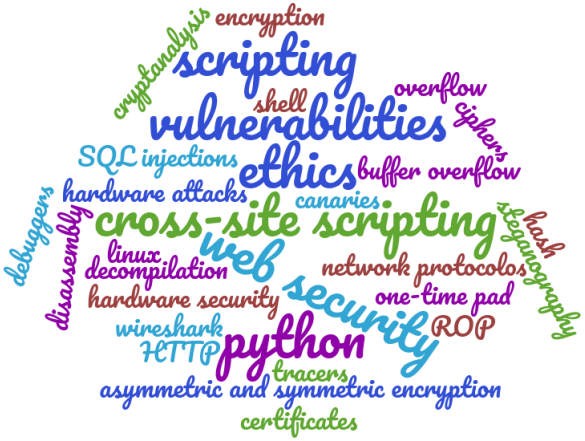
- The elephant in the room ...
- Some of you already attended
  - university courses
  - coding competitions
  - CTFs

CC.IT Training

- The elephant in the room ...
- In addition to technical skills, we seek for **team players**
  - no “first women”
  - no slackers

CC.IT Training

- 6 hours per week for 3 months
  - 2 hours of theory (including soft skills)
  - 4 hours of hands-on



CC.IT Training

- 6 hours per week for 3 months
  - 2 hours of theory (including soft skills)
  - 4 hours of hands-on

CC.IT Syllabus

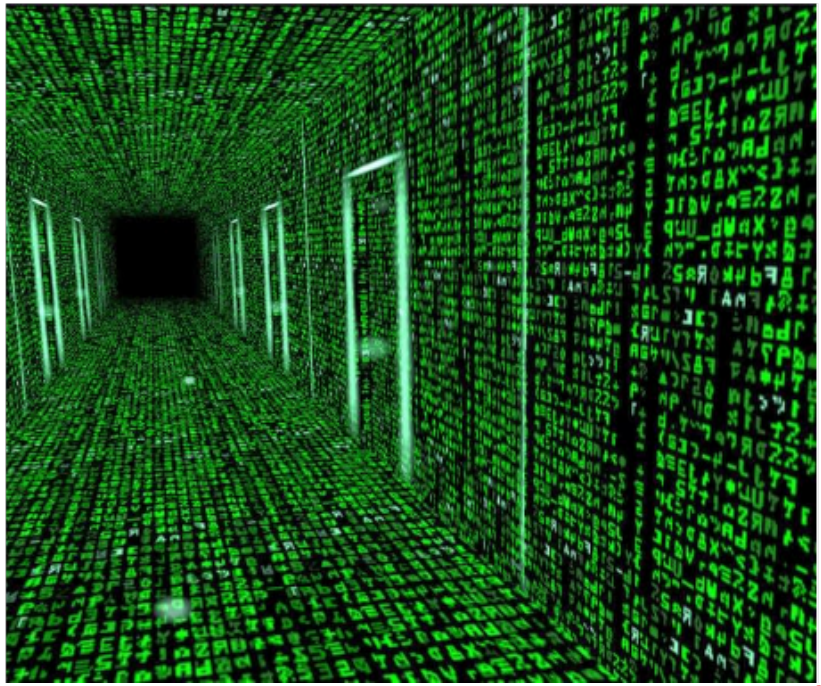
- Week #1: Introduction & Ethics
- Week #2: Network Security
- Week #3: Web Security 1
- Week #4: Cryptography 1
- Week #5: Software Security 1
- Week #6: Cryptography 2
- Week #7: Software Security 2
- Week #8: Cryptographic Protocols
- Week #9: Web Security 2
- Week #10: Software Security 3
- Week #11: Access Control
- Week #12: Hardware Security 1

CC.IT Rules

- Rules of engagement
  - After 3 consecutive absences you are out (see FAQ)
  - After too many non consecutive absences you are out
  - You will use your own laptop
  - We will provide Wi-Fi access

CC.IT Training

- You imagine it will be like this



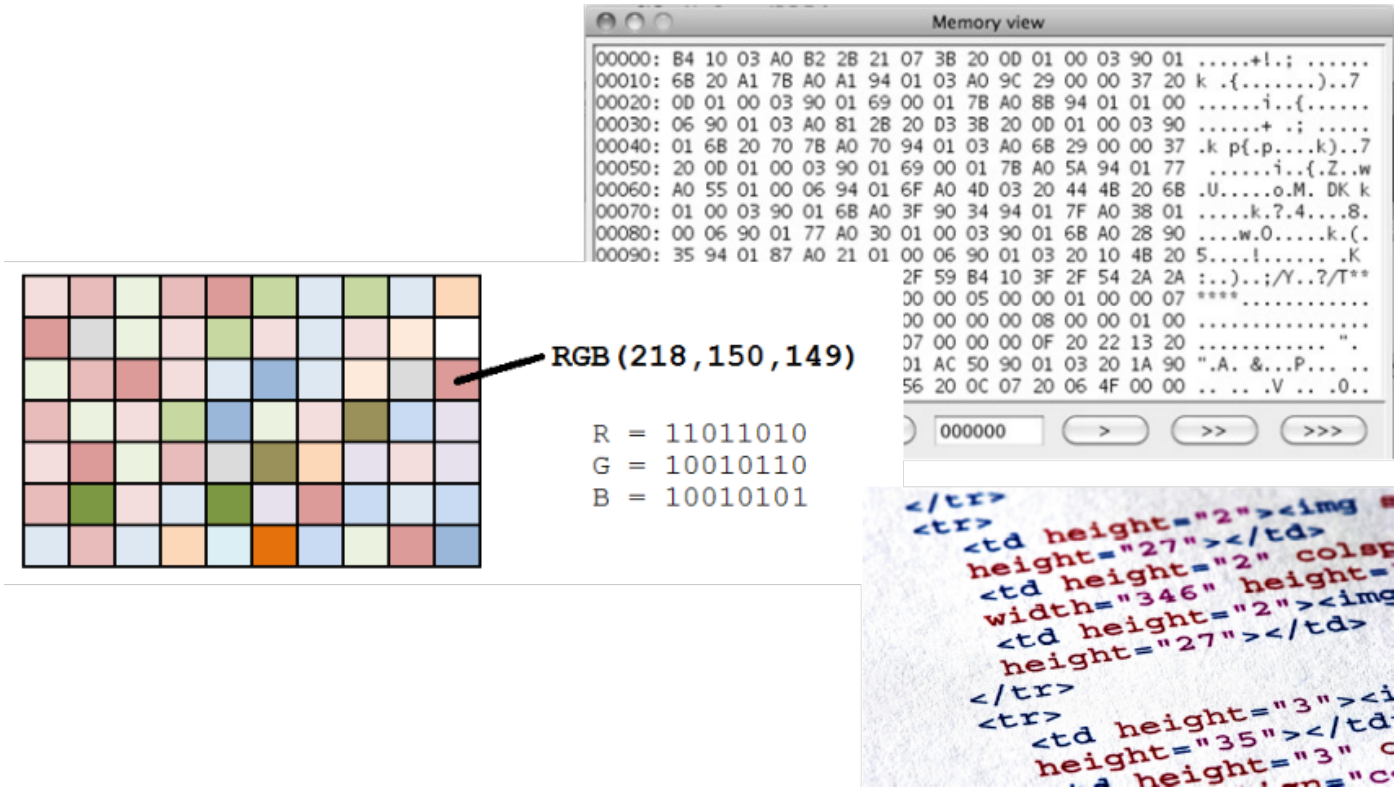
CC.IT Training

- Most often it will be like this

CC.IT Training

- But it will be fun!
- To start
  - https://ctf.cyberchallenge.it
  - Log in to check user credentials
  - Submit you first flags!

Homework: warm up challenges



CC.IT warm up

Marina Ribaudo
Università di Genova
marina.ribaudo@unige.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity
National Lab

https://cybersecnatlab.it

CYBER CHALLENGE
CyberChallenge.IT

cini
Cybersecurity National Lab

SPONSOR PLATINUM

accenturesecurity

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

B5

EY Building a better working world

eni

exprivia | ITALTEL

IBM

KPMG

LEONARDO

NTT DATA
Trusted Global Innovator

NUMERA
SISTEMI E INFORMATICA S.p.A.

Telsy

SPONSOR GOLD

bip.

cisco

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

negg

NOVANEXT
connecting the future

pwc

SPONSOR SILVER

DiGi ONE
the leading digital company

ICT CYBER CONSULTING