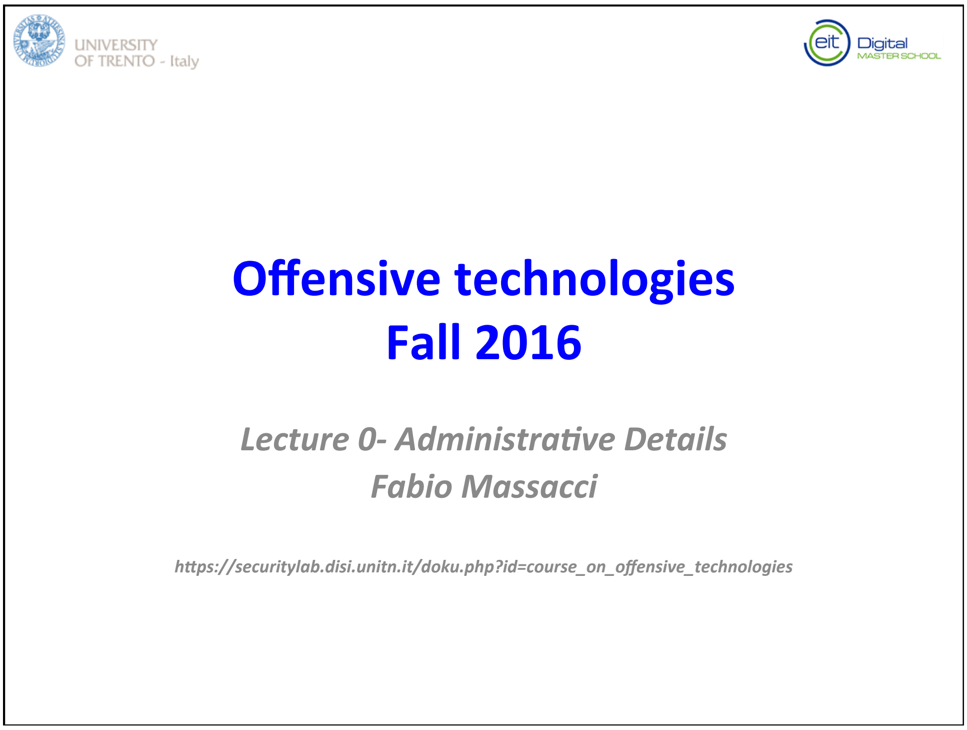


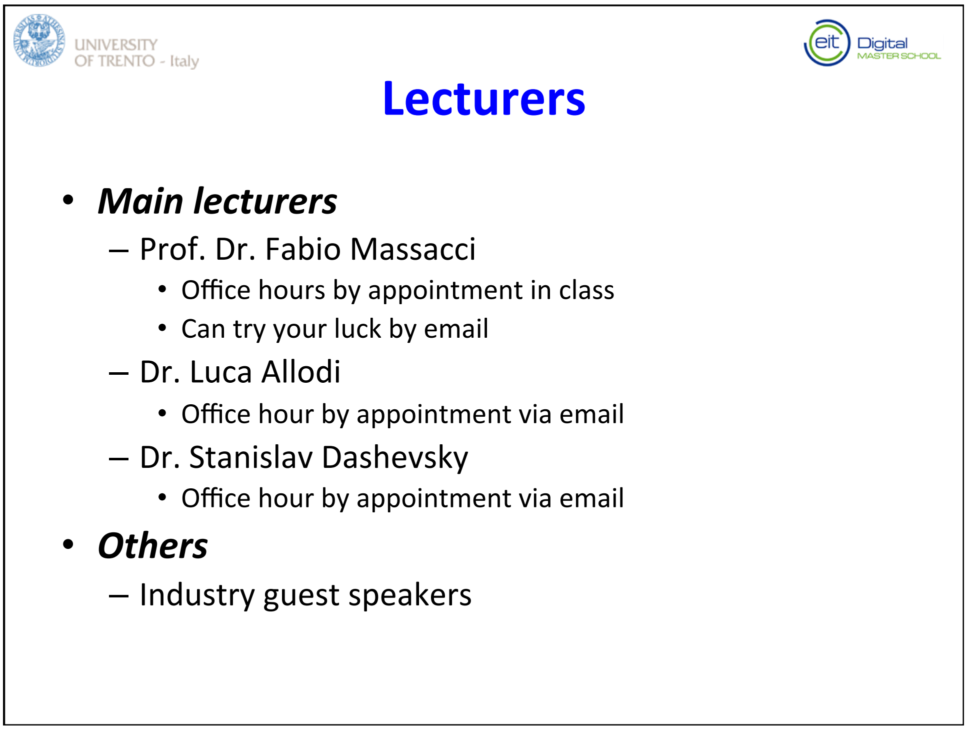
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Offensive technologies Fall 2016

Lecture 0- Administrative Details
Fabio Massacci

https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies

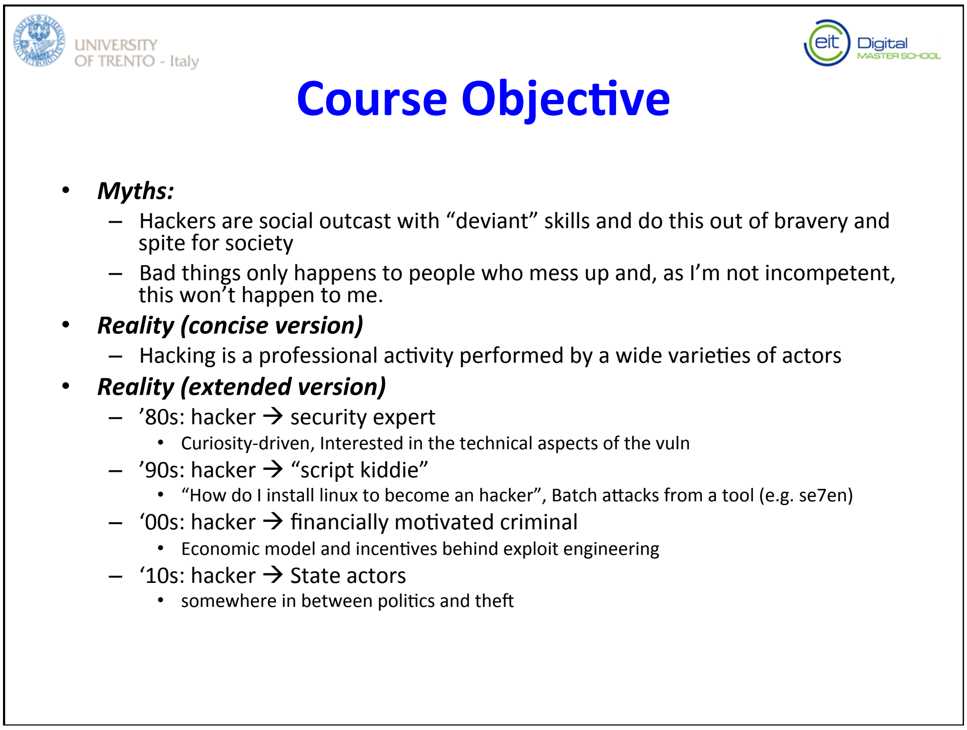


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

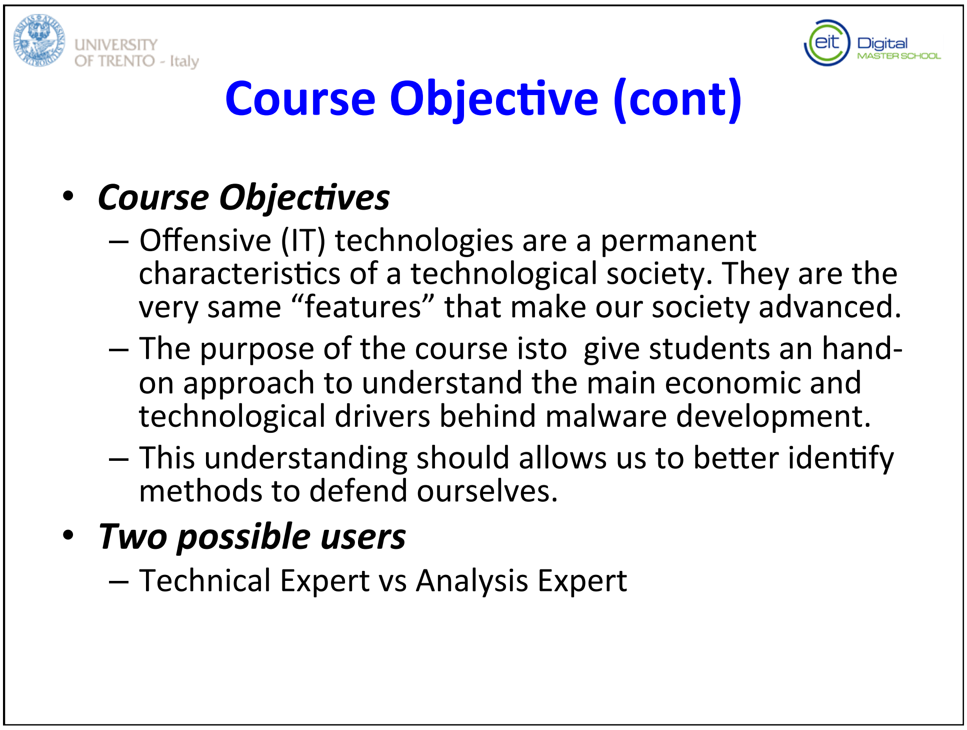
Lecturers

- ***Main lecturers***
  - Prof. Dr. Fabio Massacci
    - Office hours by appointment in class
    - Can try your luck by email
  - Dr. Luca Allodi
    - Office hour by appointment via email
  - Dr. Stanislav Dashevsky
    - Office hour by appointment via email
- ***Others***
  - Industry guest speakers



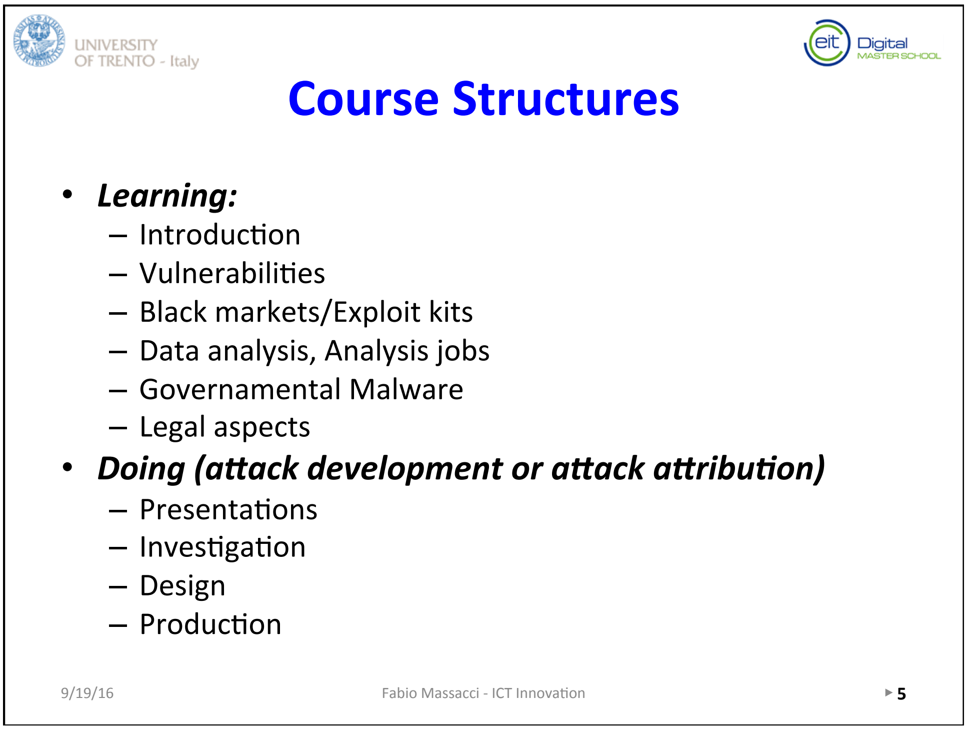
Course Objective

- ***Myths:***
  - Hackers are social outcast with “deviant” skills and do this out of bravery and spite for society
  - Bad things only happens to people who mess up and, as I’m not incompetent, this won’t happen to me.
- ***Reality (concise version)***
  - Hacking is a professional activity performed by a wide varieties of actors
- ***Reality (extended version)***
  - ’80s: hacker → security expert
    - Curiosity-driven, Interested in the technical aspects of the vuln
  - ’90s: hacker → “script kiddie”
    - “How do I install linux to become an hacker”, Batch attacks from a tool (e.g. se7en)
  - ‘00s: hacker → financially motivated criminal
    - Economic model and incentives behind exploit engineering
  - ‘10s: hacker → State actors
    - somewhere in between politics and theft



Course Objective (cont)

- ***Course Objectives***
  - Offensive (IT) technologies are a permanent characteristics of a technological society. They are the very same “features” that make our society advanced.
  - The purpose of the course isto give students an hand-on approach to understand the main economic and technological drivers behind malware development.
  - This understanding should allows us to better identify methods to defend ourselves.
- ***Two possible users***
  - Technical Expert vs Analysis Expert

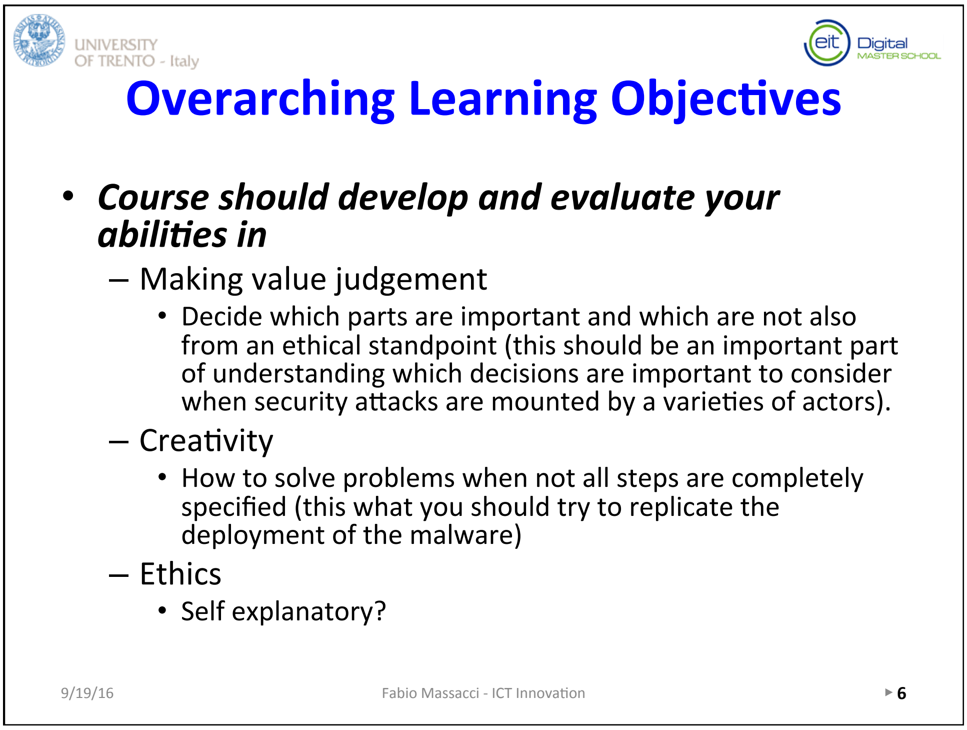


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Course Structures

- ***Learning:***
  - Introduction
  - Vulnerabilities
  - Black markets/Exploit kits
  - Data analysis, Analysis jobs
  - Governamental Malware
  - Legal aspects
- ***Doing (attack development or attack attribution)***
  - Presentations
  - Investigation
  - Design
  - Production

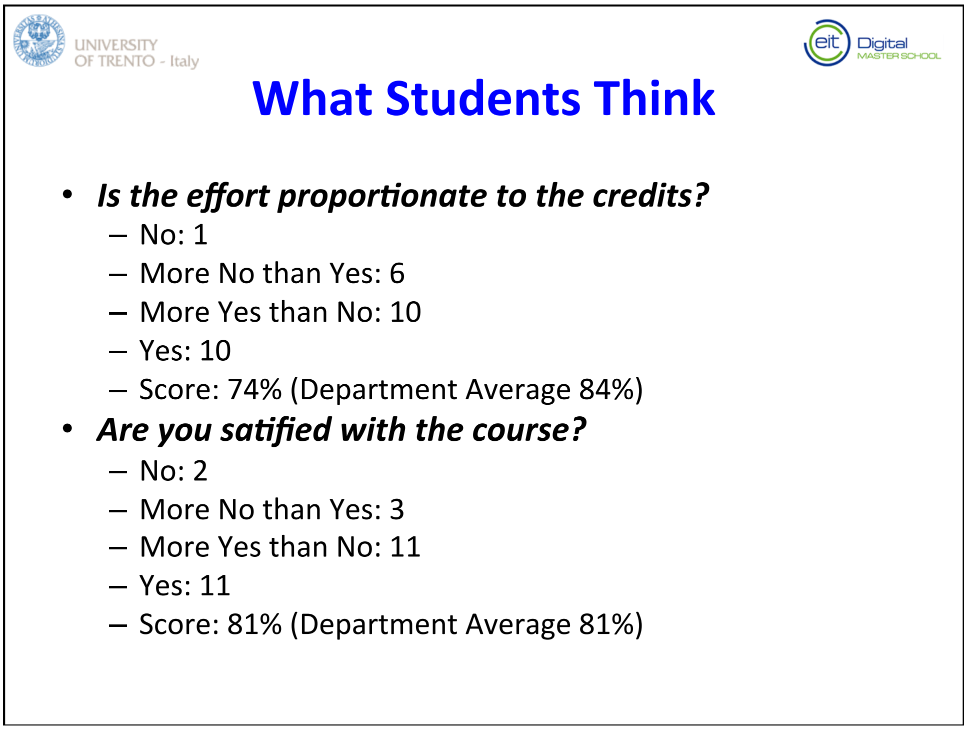


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

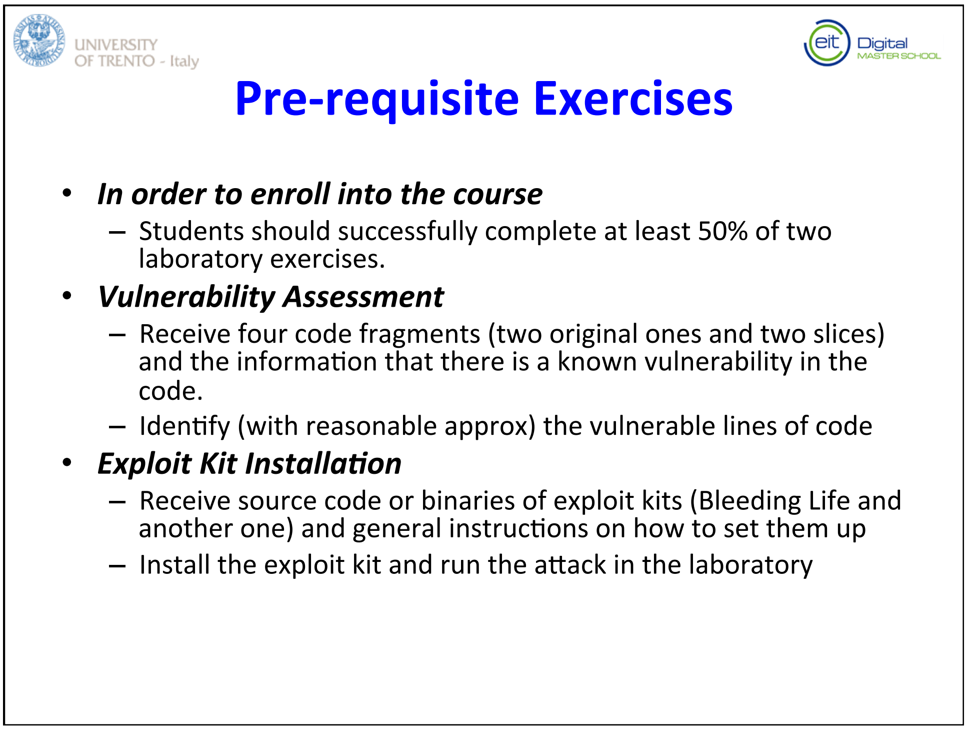
Overarching Learning Objectives

- ***Course should develop and evaluate your abilities in***
  - Making value judgement
    - Decide which parts are important and which are not also from an ethical standpoint (this should be an important part of understanding which decisions are important to consider when security attacks are mounted by a varieties of actors).
  - Creativity
    - How to solve problems when not all steps are completely specified (this what you should try to replicate the deployment of the malware)
  - Ethics
    - Self explanatory?



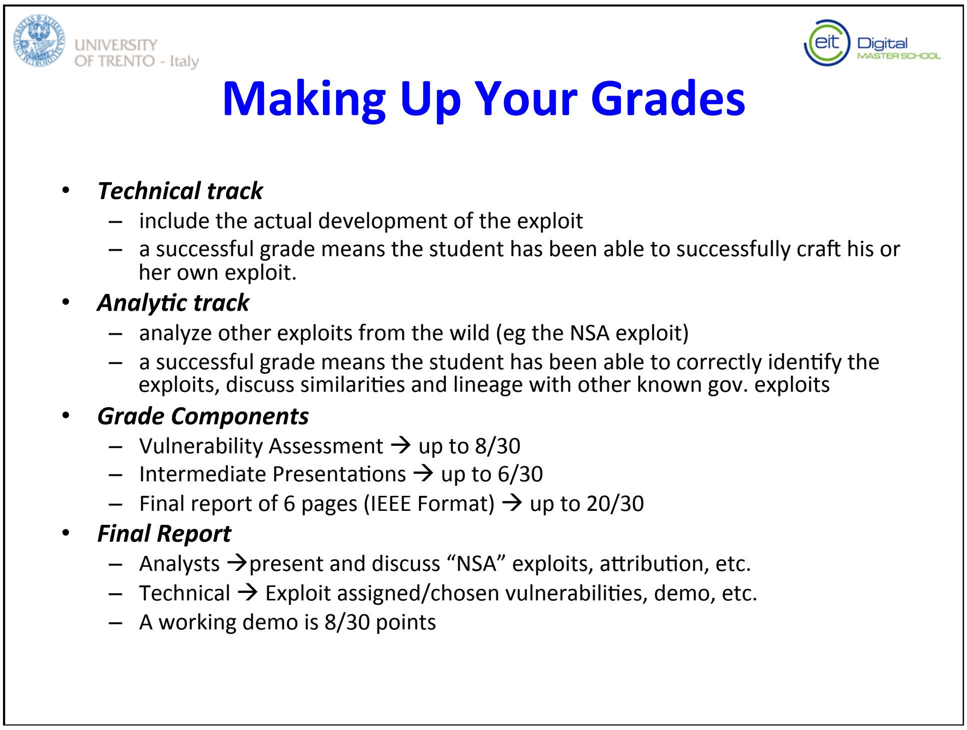
What Students Think

- ***Is the effort proportionate to the credits?***
  - No: 1
  - More No than Yes: 6
  - More Yes than No: 10
  - Yes: 10
  - Score: 74% (Department Average 84%)
- ***Are you satified with the course?***
  - No: 2
  - More No than Yes: 3
  - More Yes than No: 11
  - Yes: 11
  - Score: 81% (Department Average 81%)



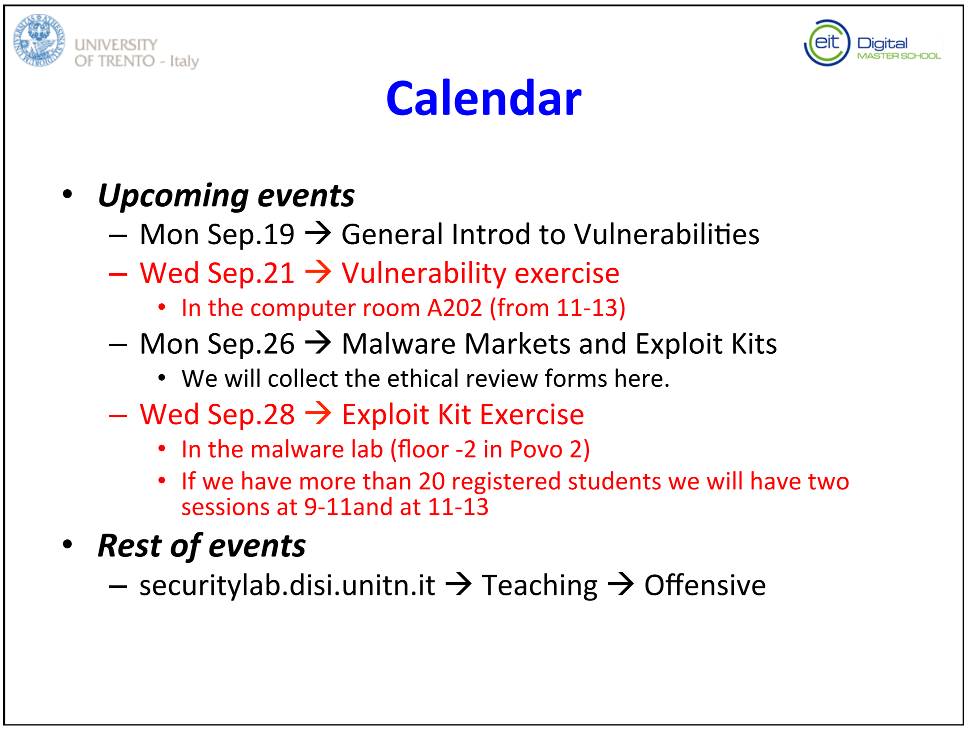
Pre-requisite Exercises

- ***In order to enroll into the course***
  - Students should successfully complete at least 50% of two laboratory exercises.
- ***Vulnerability Assessment***
  - Receive four code fragments (two original ones and two slices) and the information that there is a known vulnerability in the code.
  - Identify (with reasonable approx) the vulnerable lines of code
- ***Exploit Kit Installation***
  - Receive source code or binaries of exploit kits (Bleeding Life and another one) and general instructions on how to set them up
  - Install the exploit kit and run the attack in the laboratory



Making Up Your Grades

- ***Technical track***
  - include the actual development of the exploit
  - a successful grade means the student has been able to successfully craft his or her own exploit.
- ***Analytic track***
  - analyze other exploits from the wild (eg the NSA exploit)
  - a successful grade means the student has been able to correctly identify the exploits, discuss similarities and lineage with other known gov. exploits
- ***Grade Components***
  - Vulnerability Assessment → up to 8/30
  - Intermediate Presentations → up to 6/30
  - Final report of 6 pages (IEEE Format) → up to 20/30
- ***Final Report***
  - Analysts →present and discuss "NSA" exploits, attribution, etc.
  - Technical → Exploit assigned/chosen vulnerabilities, demo, etc.
  - A working demo is 8/30 points



Calendar

- ***Upcoming events***
  - Mon Sep.19 → General Introd to Vulnerabilities
  - Wed Sep.21 → Vulnerability exercise
    - In the computer room A202 (from 11-13)
  - Mon Sep.26 → Malware Markets and Exploit Kits
    - We will collect the ethical review forms here.
  - Wed Sep.28 → Exploit Kit Exercise
    - In the malware lab (floor -2 in Povo 2)
    - If we have more than 20 registered students we will have two sessions at 9-11and at 11-13
- ***Rest of events***
  - securitylab.disi.unitn.it → Teaching → Offensive

Material used the course

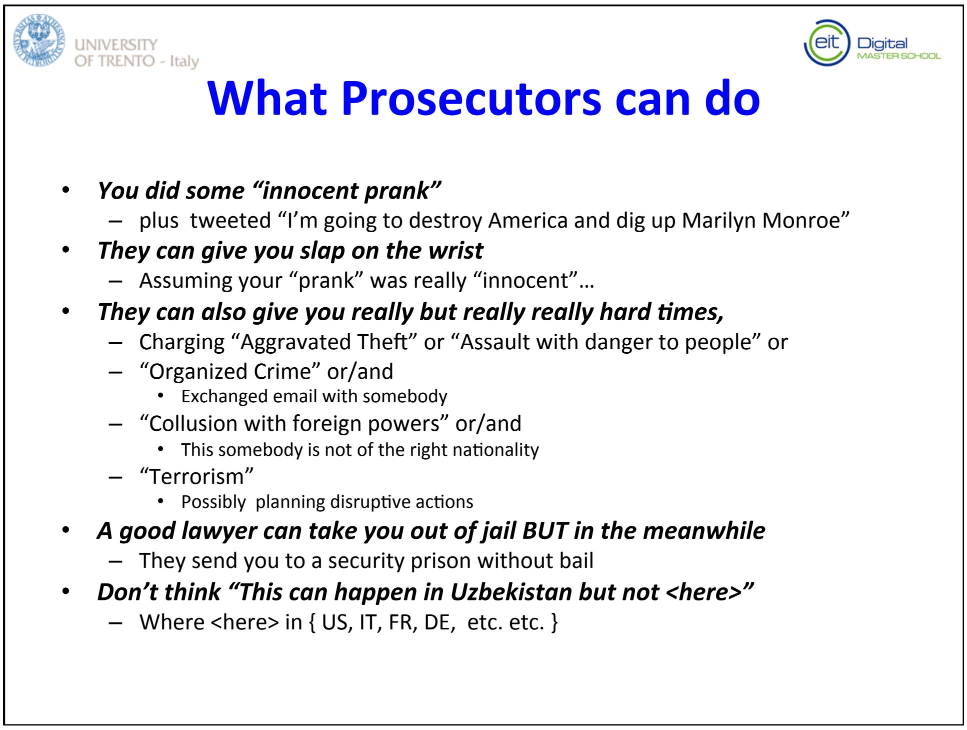
- ***MalwareLab***
  - **Malware dump** → actual malware you can try to install and test on the lab machines
  - The dump is downstairs in Povo 2 for you to analyse
- ✓ ***It is also a trove of Malware Data***
  - ✓ **Dump of emails** → insights on internal procedures of gov malware development
    - Who was the Hacking Team dealing with? What problems did their products have?
  - ✓ **Dump of bills** → insight on actual clients and malware deployment.
    - Is your own motherland government involved? If yes, how much and for what?
  - ✓ **Dump of source code** → insights on malware operations
    - Can you spot malware functionalities declared in the documentation in the actual code?

Responsible Study

- ***Material in the MalwareLab is sensitive***
  - Its content might be offensive to you (pornographic pictures, racist comments, disrespectful of your religious beliefs etc..)
  - It may create embarrassment or slander of individuals
- ***Malware is advanced tech***
  - Nobody really knows what it does (most advanced one even detect they are analyzed)
  - They can create unintended havoc when deployed out of control
  - There are mechanisms in place to prevent you from exfiltrating the data outside of lab

Ethical Acceptance

- ***You must agree to the terms and conditions of this course before having access to any data***
  - You work **only** in the lab
  - You are **not allowed** to disclose information about any individual that you find during the analysis
  - Your final deliverable, as approved by the professor is **the only public deliverable** you are allowed to disclose to third parties
- ***Any use outside the agreed framework of the course may be penally relevant (i.e. a crime)***
  - Mlab is **isolated** from rest of infrastructure → you must deliberately exfiltrate the material → cannot claim that “happened by mistake”
  - The same considerations apply if you give material to other students who have not signed the agreement → aiding and abetting = same penal responsibility as if you did it yourself.



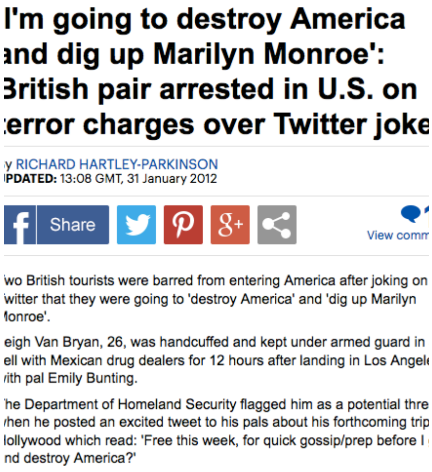
What Prosecutors can do

- ***You did some “innocent prank”***
  - plus tweeted “I’m going to destroy America and dig up Marilyn Monroe”
- ***They can give you slap on the wrist***
  - Assuming your “prank” was really “innocent”…
- ***They can also give you really but really really hard times,***
  - Charging “Aggravated Theft” or “Assault with danger to people” or
  - “Organized Crime” or/and
    - Exchanged email with somebody
  - “Collusion with foreign powers” or/and
    - This somebody is not of the right nationality
  - “Terrorism”
    - Possibly planning disruptive actions
- ***A good lawyer can take you out of jail BUT in the meanwhile***
  - They send you to a security prison without bail
- ***Don’t think “This can happen in Uzbekistan but not <here>”***
  - Where <here> in { US, IT, FR, DE, etc. etc. }

Why they are going to do it?

- ***True discussion with a (former) Judge from Italian Supreme Court***
  - **IF** a prosecutor want to investigate a computer crime (e.g. your "prank") s/he needs access to emails/internet traces etc.e tc.
  - **BUT** email is protected (this is not North Korea after all)
  - **UNLESS** there is a very serious crime going on
  - **SO** prosecutor claims "this is a very serious crime (eg Organized Crime)"
  - **THEN** judge grants access to your emails (they write to Google and Google gives them everything about your life)
  - **OBVIOUSLY** during the trial all accusations will fail as you have just done a prank (anyhow need to pay a good lawyer, technical counsel)
  - **HENCE** Prosecutor conscience is clean: no innocent people will finally be injustly condemned whilst he can investigate the bad guys
- ***Side Effects…***
  - **WISELY** "charges of serious crimes" go hand in hand with measures limiting offenders (eg you won't let a mafios go around and kill more people)
  - **BUT NOW** you are charged with the same crimes of the dangerous mafioso…
  - **SO** police sends you in a security prison without bail as potential offender…

You don't believe it, do you?



I'm going to destroy America ınd dig up Marilyn Monroe': 3ritish pair arrested in U.S. on :error charges over Twitter joke

y RICHARD HARTLEY-PARKINSON
PDATED: 13:08 GMT, 31 January 2012

wo British tourists were barred from entering America after joking on witter that they were going to 'destroy America' and 'dig up Marilyn lonroe'.

eigh Van Bryan, 26, was handcuffed and kept under armed guard in ell with Mexican drug dealers for 12 hours after landing in Los Angel ith pal Emily Bunting.

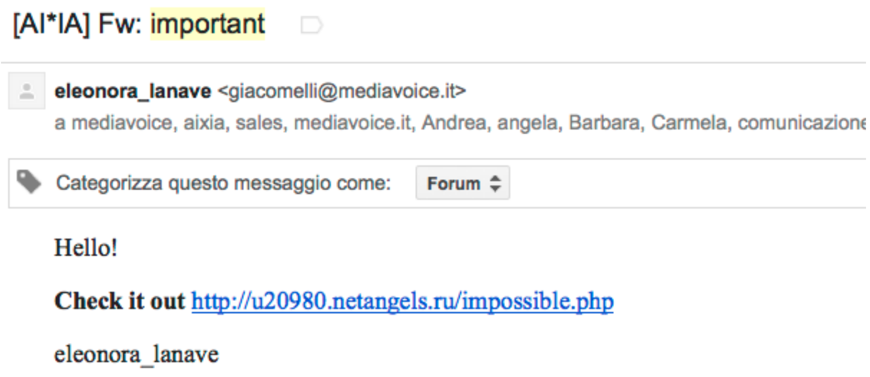
he Department of Homeland Security flagged him as a potential thre hen he posted an excited tweet to his pals about his forthcoming trip lollywood which read: 'Free this week, for quick gossip/prep before I nd destroy America?'

- ***Leigh, from Coventry, and Emily, 24, from Birmingham, were then quizzed for five hours at LAX before they were handcuffed and put into a van with illegal immigrants and locked up overnight.***
  - "When we arrived at the prison I was shoved in a cell on my own but after an hour two huge Mexican men covered in tattoos came in and started asking me who I was.
  - 'They told me they'd been arrested for taking cocaine over the border.
  - 'When the food arrived on the tray they took it all and just left me with a carton of apple juice.'"
- ***They spent 12 hours in separate holding cells before being driven back to the airport where they were put on a plane home via Paris.***

Rules of Engagement

- ***Asking questions in class is always the best policy***
  - Your colleagues may be interested in the answer
  - Things are easier to explain
  - The prof gets hundreds email per day…
    - Today before 10:30 am (emails and counting)
- ***Do your homework first***
  - "I can't bother to find the answer, I will ask the prof."
    - Q: "I don't remember to whom the deliverable should be submitted"
    - A: "read my slides"
- ***Write with "[OffTech]" in the subject***
  - "important" is a no go
  - "urgent" is not better

Important Messages…



[AI*IA] Fw: important

eleonora_lanave <giacomelli@mediavoice.it>

a mediavoice, aixia, sales, mediavoice.it, Andrea, angela, Barbara, Carmela, comunicazione

Categorizza questo messaggio come: Forum

Hello!

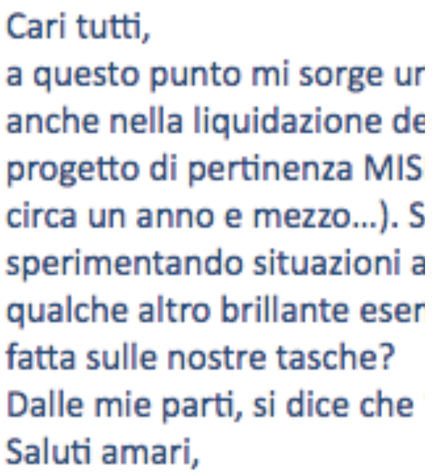
Check it out http://u20980.netangels.ru/impossible.php

eleonora_lanave

UNIVERSITY
OF TRENTO - Italy

eit Digital
MASTER SCHOOL

Urgente…



Cari tutti,

a questo punto mi sorge ur

anche nella liquidazione de

progetto di pertinenza MIS

circa un anno e mezzo…). S

sperimentando situazioni a

qualche altro brillante eser

fatta sulle nostre tasche?

Dalle mie parti, si dice che

Saluti amari,

- ***Essentially 28 guys moaning that the Ministry is not paying their reviews.***
- ***They keep "updating" each other on the status***
- ***I don't even know why Google returns it when I searched "urgente" in my mailbox***
  - (first hit)
- ***First mail was 2yrs ago… I answered that one.***