Network Security

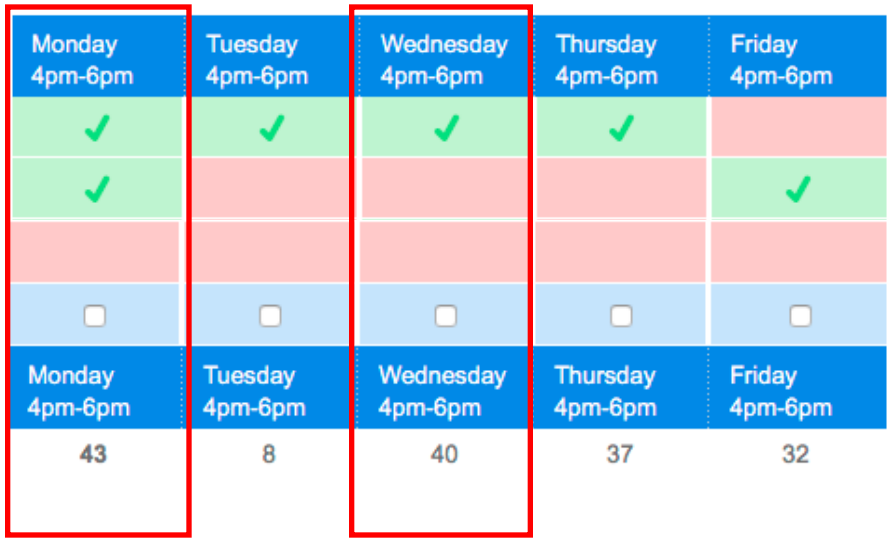
AA 2015/2016

Lab activities

Dr. Luca Allodi

Laboratories

- Laboratory room holds ca. 40 people
  - We need to split the class in half
- Each day is divided in two sessions
  - Morning session → attended by students that have NOT indicated a preference for the evening in the Doodle
  - Evening session → attended by students that DID indicate a preference for the evening in the Doodle



Laboratory organisation

- Each session is a **two hours** session
  - The complexity of the lab must match length of session
    - Too many things to do → nobody will finish
    - Keep it simple, but not simplistic
- We need two groups per laboratory topic
  - Group A does the lab in the morning
  - Group B does the lab in the evening
    - All group members must attend
- Laboratories A and B are developed **independently**
  - Same topic but original development

Choosing a lab topic

- I propose you **n/2 topics** for the lab, with **n=no. of groups**
  - At the moment n=20
  - Topics assigned on a first-come first-served basis
    - Starting at noon Wednesday, 9th of March
    - Double-booking will be re-assigned by me
  - **Some of you asked to pre-book a lab topic. In fairness to other students, please book your topic starting tomorrow.**
- If you want to propose your own topic for the lab, you must find a "sibling group B" that will develop the second session
  - Subject to approval from me
    - e.g. Want to do a lab on malware reverse engineering?
      1. Where do you get IDA Pro-equivalent from?
      2. What malware?
      3. Can you fit the lab in 2 hours?
         - If yes, will people be able to follow?

Lab topics - proposals

- Network attacks
  1. ARP Poisoning + TCP session hijacking
  2. Denial of service (ICMP flood, SYN, UDP, .., MitM RST)
  3. DNS cache poisoning + Kaminsky
- Software attacks
  4. XSS + phishing/CSRF
  5. Buffer Overflows
  6. SQLi + defenses
- Defenses
  7. FW (stateless) → allows/blocks/redirects/forwards packets depending on pre-defined rules
  8. FW (stateful) → FW whose rules consider connection states
  9. NIDS – Snort → network sensor that detects possible attacks by matching pre-defined signatures with network traffic
  10. NIDS – Bro → like above but more expressive languag (can define more complex signatures)

Lab procedure and deadlines

- You can develop your lab activity on your own laptop or in the laboratory downstairs
- Laboratories must be **fully autonomous**
  - Virtualised infrastructure
    - To replicate the lab it is sufficient to load the VMs
- Laboratories are delivered in the order of the topics chosen for the classes
  - This is to keep workloads balanced among all groups
    - Network goes first → starting on the 20th April
    - Software goes second
    - Defense goes third
- Labs should be ready a week before the deadline
  - This is so that you have time to configure the machines downstairs

Lab deliverable and grading (17 points)

- Each lab must be delivered with
  1. A full report describing the activity in detail
     - Deadline = day of lab
  2. Slides that will be used during the presentation
     - Deadline = 3 days before the lab
       - Participants can have a look beforehand at what will the activity be about

+ 7 points
Same score for all group members

- All students did 1/3rd of lab → +2
- All students did 2/3rd of lab → +4
- All students did 3/3rd of lab → +4

+ 10 points

This is individual

- Group members that do not help during the lab/are not present get none of these 10 points
- Grade is balanced w.r.t. no. of group members

Lab - notes

- The intent of these laboratories is twofold:
  - Give the opportunity to each group to study in detail a specific topic
  - Give the opportunity to everybody to see "a little bit of everything"
    - The goal of the labs is not to make everyone an expert
      - Don't overdo it → put everything you learned in the report, not in the lab
- A good laboratory has the following properties:
  1. Make sure that participants know what the next step will be
     - This is the reason why I ask the slides a few days early
     - Must also emerge from how your activity unfolds in the lab
  2. Start off with easy tasks, complexity must emerge at the rate of "easy steps"
     - *Divide et impera*