Network Security

AA 2020/2021

Lab Activities

Malware LAB

- Due to restrictions as consequence of the Covid-19 we transformed the malware lab in a virtual lab
- So instead of using the Malware Lab, the lab will be prepared and performed on the student's computer
- Each group will do the presentation online using Zoom in synchronous mode and all students must participate to the online meeting

Laboratory organisation

- Each session is a full (105-120 minutes) online lecture
- The complexity of the lab must match the length of session
  - Too many things to do → nobody will finish
  - Keep it simple, but not shallow
- All group members must attend
  - All students are recommended to attend (we collect signatures)

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

Lab topics

- Deadlines match the reported order
- Network attacks
  1. ARP Poisoning +MitM attacks + TCP session hijacking
  2. DNS cache poisoning and Kaminsky attack (w/ network simulator)
  3. Key Reinstallation Attack and mitigation

- Software attacks
  4. Email and Social media phishing

- Vulnerability Analysis
  5. Vulnerability assessment - OpenVAS
  6. Penetration testing - Metasploit 1
  7. Penetration testing - Metasploit 2

- Defenses
  8. FW → allows/blocks/redirects/forwards packets depending on pre-defined rules, including rules consider connection states and stateless
  9. NIDS – Snort → network sensor that detects possible attacks by matching pre-defined signatures with network traffic
  10. NIDS – Zeek → focus on network analysis. It looks for specific threats and trigger alerts (can define more complex signatures)
  11. Honeypot
  12. Vulnerability Management Lifecycle (TheHive, Wazuh)
  13. Reverse Engineering

Lab procedures 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
  - Instructions on how to load VM will be published in classroom
- Laboratories are delivered in the order of the topics as presented in the classes
- This is to keep workloads balanced among all groups
  - Network goes first
  - Software goes second
  - Defense goes third
- Labs should be ready days before the deadline
  - This is so you have time to set the online lecture and let students to configure the VM on their computer (see deadlines)

Lab deliverable and grading (12 points)

- Each lab must be delivered with

1. A full report (maximum 20 pages) describing how to replicate the activity in detail
   - Deadline = within 6 days after the day of lab

+ 5 points
Same score for all group members

2. Slides that will be used during the presentation
   - Deadline = 2 days before the lab
   - VM should be distributed 6 days before the day of the lab.
   - Participants can have a look beforehand at what will the activity be about

+ 7 points
Individual score. All group members must present

Grading criteria for the presentation

- Organization (time, flow of different topics covered, consistency, etc.) 25%
- Content and structure (quality of the content, how excersices are structured, etc.) 30%
- Graphical and visual elements 20%
- Presentation skills 25%