Vulnerability assessment

A quick exercise before we get started

Luca Allodi

What this session is and is not

- This is an exercise to see how intuitive it is for you to evaluate **vulnerability criticality**
- This is **not** an exam and will **not** in **any** way influence your final vote
- I will give you a sheet of paper with 30 vulnerabilities and their description
  - This is what who makes the assessment has at his disposal at the start of the process
- I will ask you to grade the vulns according to a number of metrics and to express
  - Your “gut feeling” on the severity of the vulnerablity
  - Your confidence with your assessment

Vulnerabilities

- Are bugous pieces of code in a software
- Can be exploited to deviate software's execution from its designed behavior
- There are of many types
  - Buffer overflows
  - Authentication
  - XSS
  - …
- At this stage you are NOT required to know any of this

How to grade vulnerabilities? (1)

- There is a standard for that: the CVSS
- It is now at its third revision, under construction
- CVSS is the **worldwide standard** used for
  - Credit card security
  - Security mangement by U.S. National Institute of Standards Technology (e.g. SCAP)
  - Security communication by ISO standards (e.g. ISO 29147)
  - ….
- I am one of the authors of the standard
  - Been working with CISCO, Intel, IBM and many others on its definition
  - I am thoroughly biased on its interpretation

How to grade vulnerabilities? (2)

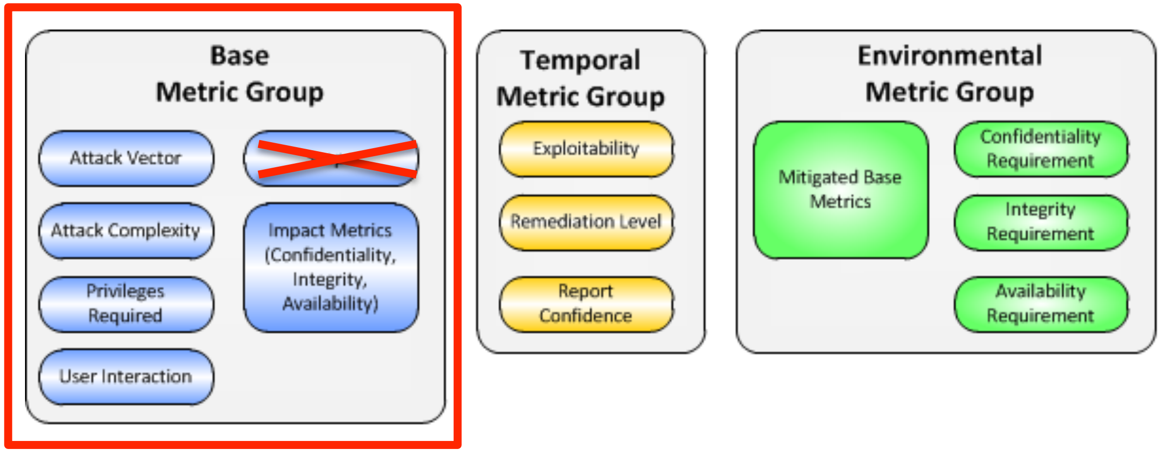
- I will **not** tell you how to interpret the metrics
- I will rather just introduce you very briefly to how the CVSS works
- You will do the rest by yourself

- I'll give you about 45 minutes to get at it
- Then we will resume the "original" lecture

- This experiment will be repeated at the end of the course
  - This will tell us how much a security background influences the use of the standard
  - In the real world, it is **not** security experts that do it
    - But rather system administrator or general IT staff (e.g. CERTs)

The Common Vulnerability Scoring System (1)

- CVSS is based on a number of metrics



- We will use the base metric group
- And not all of them

The Common Vulnerability Scoring System (2)

- Attack Vector
  - Network, Adjacent, Local, Physical
- Attack Complexity
  - High, Low
- Privileges required
  - High, Low, None
- User interaction
  - Required, None
- (Impacts on) Confidentiality, Integrity, Availability
  - Complete, Partial, None
- Severity: 1-10 with 10 very bad, 1 not so bad
- Confident? Yes=the vuln is clear to me; No= I'm not sure

The Common Vulnerability Scoring System (3)

- It evaluates each metric relative to the **vulnerable component**
  - A vulnerability in a **database** must be evaluated relative to what it allows the attacker to do on the **database**
  - Example description (invented): *Misconfiguration in OracleDB allows attacker to spawn a root shell on the system and gives local access to DB*
    - The vulnerable component is the **database**
    - What does it do **to the database**?