Dradis

Daniel Martín Gómez

etd

september '07

Agenda

→ Scenario: where are we?

→ System design

→ Architecture

→ Implementation

→ Demo

→ What's next?

➔ Penetration testing is about <u>information</u>

Information Discovery

✔ port scan
✔ vuln. scan
✔ web app scan
✔ ... **SEMS**

Exploiting

✔ metasploit
✔ milw0rm
✔ ...

Reporting

✔ reporterator
✔ word
✔ pdf tools
✔ ... **Repor2rator**

➔ ~~Penetration testing is about~~ [information](#)

➔ And what about information sharing?

- ✔ Each tester writes a "notes" file
- ✔ Some testers add the stuff straight to reporterator

Problems with this approach:

- ✔ Exploiting oportunities may be lost
- ✔ Overlapping
- ✔ Lack of standarization in the "notes"
- ✔ Synchronization problems when using reporterator

➔ ~~Penetration testing is about information~~

➔ And what about information sharing?

    ✔ Each tester writes a "notes" file

    ✔ Some testers add the stuff straight to reporterator

    Problems with this approach:

        ✔ Exploiting oportunities may be lost

        ✔ Overlapping while testing

        ✔ Lack of standarization in the "notes"

        ✔ Synchronization problems when using reporterator

Does this sound anywhere near **Quality** or **Efficiency**?

What is DRADIS?

Agenda

→ ~~Scenario: where are we?~~

→ System design

➜ **Goals and chalenges**

  ✔ create a system to effectively share information

➔ Goals and chalenges

- ~~create a system to effectively share information~~
- easy to use, easy to be adopted

➔ Goals and chalenges

- ✔ ~~create a system to effectively share information~~
- ✔ ~~easy to use, easy to be adopted~~
- ✔ flexibility => growth ; good design

➔ Goals and chalenges

- ~~create a system to effectively share information~~
- ~~easy to use, easy to be adopted~~
- ~~flexibility => growth ; good design~~
  - ✔ small and portable, so it can be used on site

- ~~Goals and chalenges~~
  - ~~create a system to effectively share information~~
  - ~~easy to use, easy to be adopted~~
  - ~~flexibility => growth ; good design~~
  - ~~small and portable, so it can be used on site~~

➔ Benefits
  ➔ information is organized

- ~~Goals and chalenges~~
  - ~~create a system to effectively share information~~
  - ~~easy to use, easy to be adopted~~
  - ~~flexibility => growth ; good design~~
  - ~~small and portable, so it can be used on site~~

➜ Benefits
  ➜ information is organized
  ➜ saves time: while testing and while reporting

- ~~Goals and chalenges~~
  - ~~create a system to effectively share information~~
  - ~~easy to use, easy to be adopted~~
  - ~~flexibility => growth ; good design~~
  - ~~small and portable, so it can be used on site~~

➔ Benefits
  - ➔ ~~information is organized~~
  - ➔ ~~saves time: while testing and while reporting~~
  - ➔ effective knowledge sharing

→ Goals and chalenges

- create a system to effectively share information
- easy to use, easy to be adopted
- not too restrictive
- flexibility => growth ; good design
- small and portable, so it can be used on site

→ Benefits

→ information is organized

→ saves time: while testing and while reporting

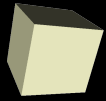→ effective knowledge sharing
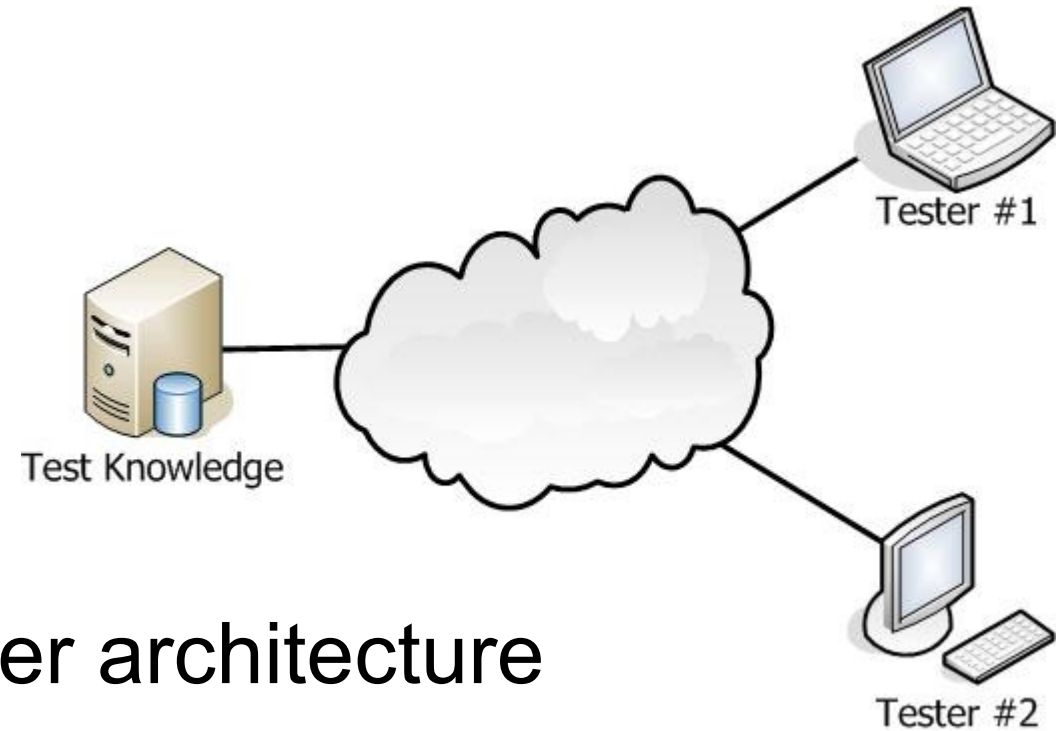
→ it is also good for one man testing

Agenda

→ ~~Scenario: where are we?~~
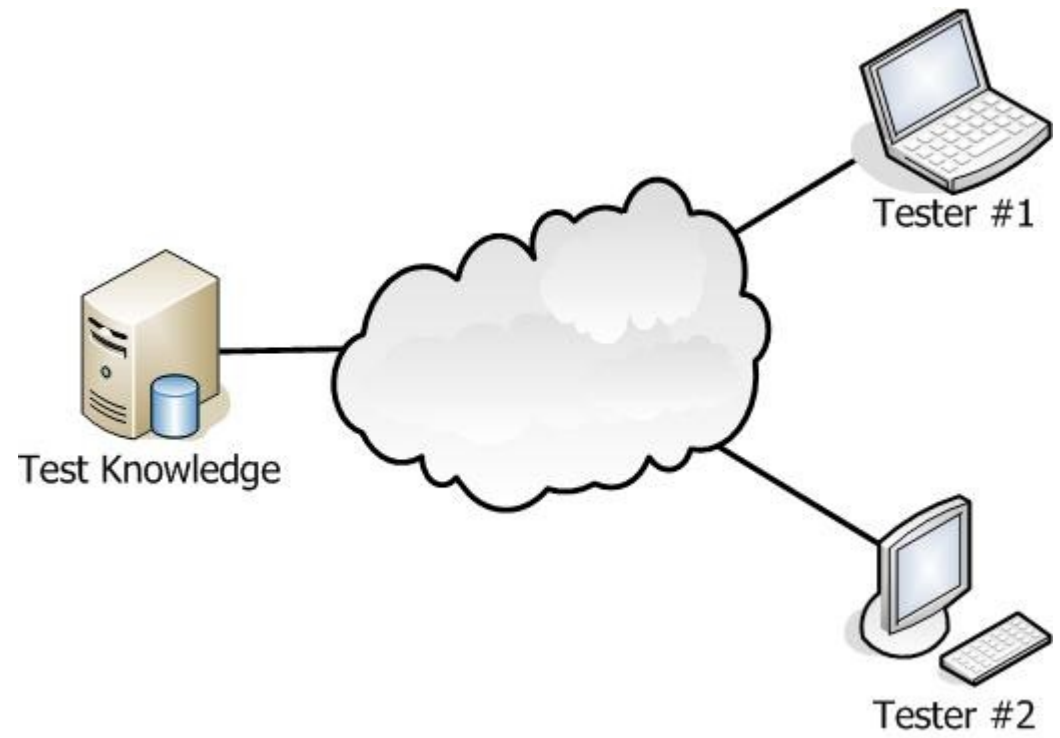
→ ~~System design~~

→ Architecture

DRADIS

Test Knowledge

Tester #1

Tester #2

- ➜ Client / Server architecture
- ➜ Coded in Ruby
- ➜ Multiple interfaces
- ➜ Different user profiles

MySQL

SQLite

RAILS

Database

REST

Web

Test Knowledge

Tester #1

Tester #2
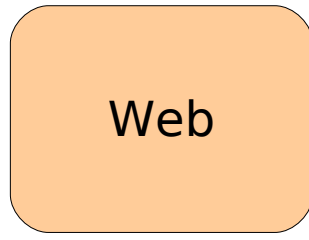
Ruby
A Programmer's Best Friend

Agenda

→ ~~Scenario: where are we?~~

→ ~~System design~~

→ ~~Architecture~~

→ Implementation

Agenda

→ ~~Scenario: where are we?~~

→ ~~System design~~

→ ~~Architecture~~

→ ~~Implementation~~

→ Demo

Agenda

→ ~~Scenario: where are we?~~

→ ~~System design~~

→ ~~Architecture~~

→ ~~Implementation~~

→ ~~Demo~~

→ What's next?

- Give it a try!
- Feature requests
- Improve it yourself

DRADIS

- It will be released under GPL
- Hopefully on sourceforge

22

¿Questions?

Daniel Martín Gómez
etd

september '07