TEACHING SECURITY WITH INTERACTIVE EXERCISES

Richard Weiss
The Evergreen State College
2700 Evergreen Parkway, NW
Olympia, WA 98505
weissr@evergreen.edu

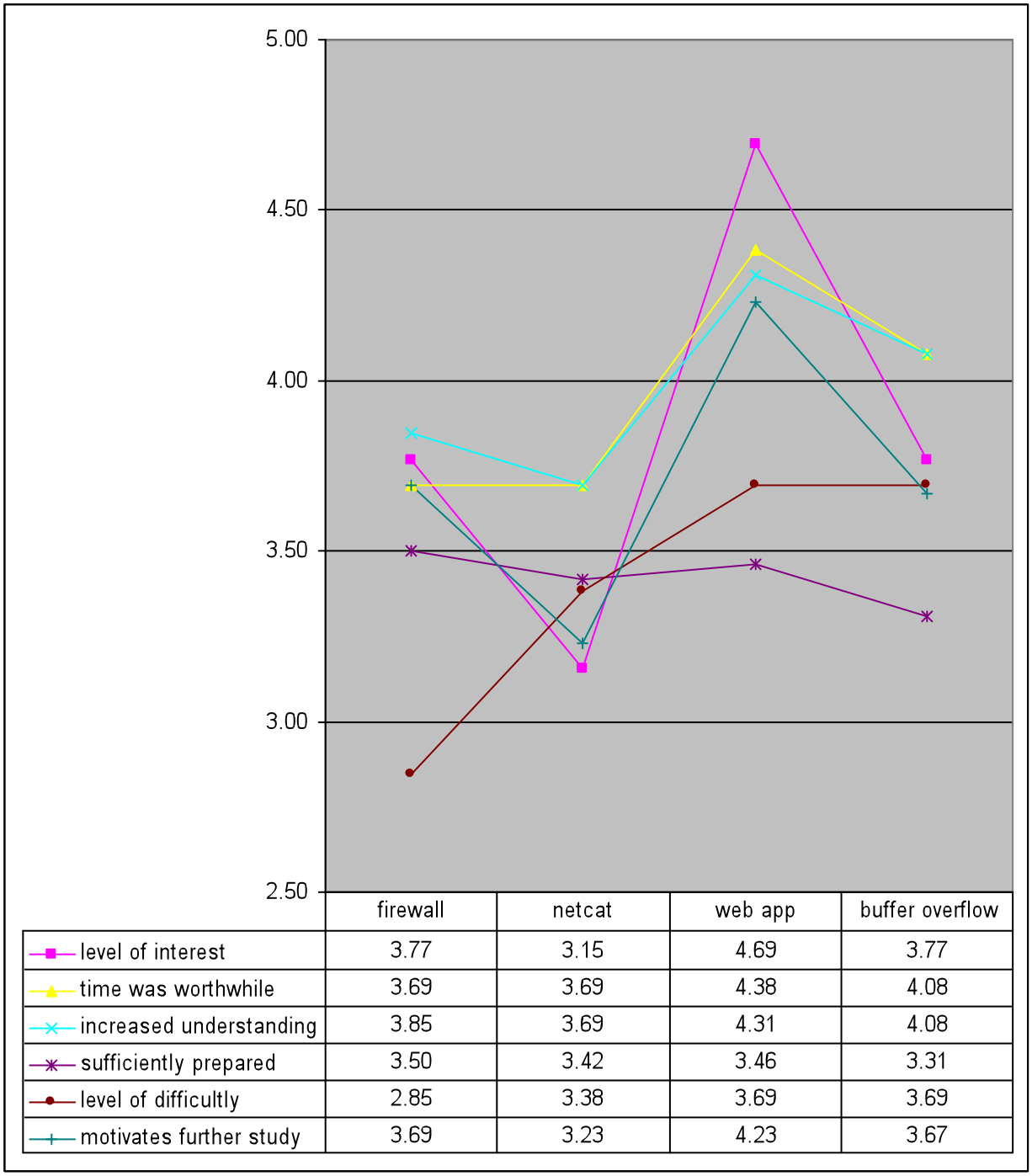
Jens Mache
Lewis & Clark College
Portland, OR 97219
jmache@lclark.edu

ABSTRACT
Teaching cyber security is becoming an important part of the undergraduate computer science curriculum, and it is receiving increased attention nationally in the proposed ACM/IEEE CS2013 Curricula Guidelines. Since many students seem to prefer hands-on experience, we have evaluated a small sample of interactive exercises. These exercises were used in undergraduate classes at two colleges (The Evergreen State College and Lewis & Clark College). We show the results of the surveys we gave to the students and the features of those exercises with strengths and weaknesses from the perspectives of both the students and instructors. We examine each for the fundamental security principles that are covered. We also consider how these exercises could be included in standard core courses such as networks, computer architecture, database systems, or software engineering.

INTRODUCTION
There are some cybersecurity exercises available online to educators, including SEED [1] and Security Injections[5]. Nevertheless, there are significant challenges to setting up a class laboratory with interactive exercises. Here are some of the problems that instructors can face:

1. Instructors may not have time to learn all of the background, and the exercises don't include background material such as tutorials on skills and tools.
2. Instructors may not have the expertise to answer detailed questions that students might ask.
3. The exercises require manual configuration of VMs and networks.
4. The exercises don't integrate with other course material
5. Exercises don't have formative or summative assessment questions.

METHODOLOGY AND RESULTS
What we did: Over three years, the two authors taught undergraduate cybersecurity courses and incorporated a number of interactive exercises, some of which were competitive. We evaluated the exercises using surveys towards the end of each course.
Below figure shows some of the results from the 2011 survey at Lewis & Clark College. Two popular competitive exercises were (1) breaking into a “banking” web application and (2) a firewall simulation [4]. Students thought that a buffer overflow exercise [1] (which integrates well with Erickson's text [2]) was difficult, but that it increased their understanding.
In the 2012 version of our classes, we also used a recent Lab Manual [3] and the RAVE environment. RAVE was already configured for these exercises, so there was no setup required by the instructors. We also developed a denial of service exercise of our own. We will report on the results from the 2012 survey which was given at both schools.



	firewall	netcat	web app	buffer overflow
level of interest	3.77	3.15	4.69	3.77
time was worthwhile	3.69	3.69	4.38	4.08
increased understanding	3.85	3.69	4.31	4.08
sufficiently prepared	3.50	3.42	3.46	3.31
level of difficultly	2.85	3.38	3.69	3.69
motivates further study	3.69	3.23	4.23	3.67

BIBLIOGRAPHY

[1] Du, W., www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/. retrieved 9/10/2012
[2] Erickson, J., *Hacking: The Art of Exploitation,* San Francisco, CA: No Starch Press, 2008.
[3] Nestler, V., White, G., Conklin, W.A., Principles of Computer Security: CompTIA Security+ and Beyond, Lab Manual. McGraw Hill, 2011.
[4] Williams, K., http://williams.comp.ncat.edu/firesim, retrieved 9/10/2012.
[5] Turner, C.F., Taylor, B., Kaza, S. Security in computer literacy – A model for design, dissemination, and assessment. *SIGCSE'11* . Website: http://triton.towson.edu/~cssecinj/