

CSE694X: Applied Information Security Projects

Steve Romig and Dong Xuan

Feb. 13, 2008

A. Overview

B. Student Evaluation

C. Proposed Changes

D. Final Remarks

Appendix (Syllabus, SEI and SET scores)

A. Overview

Course Description

Team-based projects: solve information security challenges (host/network hardening, intrusion detection and vulnerability scanning, forensics) in virtual server environment; results communicated through report writing and presentation.

Highlights

- The course was taught in Fall 2007
- Three projects (1) Host Hardening Project, (2) Firewall, Intrusion Detection, and Scanning Project and (3) Forensics. These three projects were run sequentially, rather than in parallel
- Three guest lectures on security practices in real-world
- 17 attendees: students: 7 graduates, 9 undergraduates and 1 visitor (auditing); two females
- Good student evaluations

B. Student Evaluations

B.1. Summary of the SET and SEI Results

Our overall SEI rating was 4.9 (out of 5).

The SET results are harder to summarize. Our best score was 1.1 (for both "Instructor possessed thorough knowledge of course subject area" and "Given the opportunity, I would choose this instructor for another course.") Our worst score was 1.9 ("Course grading policies were clear." and "Compared with other courses, my effort for this course was:").

According to the comments that the students made on their SETs, they liked the real-world and hands-on nature of the projects (5 and 6 comments about these, respectively) and the knowledge and approachability of the instructors (6 comments). They also liked working in groups and the guest lectures.

The single largest criticism was that we need more hardware resources for the course. Remote access was painfully slow (especially for Unix virtual machines) and we sometimes didn't have enough remote access machines for everyone. We were constantly running low on disk space and it was difficult to manage disk space since the disk resources would sometimes become disconnected from the virtual environment, which the students couldn't clean up.

B.2. Our Own Survey

We also conducted our own survey asking more specific questions about the 3 projects. We only received responses from 7 of the students unfortunately, but what we got was consistent with what we learned through the SET results.

The projects were open-ended in that we gave them a list of 8-10 objectives and asked them to try to finish at least the first 3 or 4 (and add more if they wanted more of a challenge). Most people seemed to have gotten some personal experience with most of the 3 or 4 basic objectives for each project, which is good. One person commented that they would have liked more challenging projects (though I know that they didn't complete all of the objectives laid out for the projects :-), and one person commented that they would have liked simpler projects (though I don't know how we could have made it any simpler!).

C. Proposed Changes

1. **More lectures.** We used about one-third of the class sessions as in-class labs for the students to work. The students expressed great interest in more lectures, both from the instructors and from guest-lecturers. More lectures would also give us more opportunities to integrate the hands-on projects with a broader background of knowledge about Information Security (e.g. building on what they would have learned in CSE 551 if they had taken it already).

2. **More disk space.** Disk space became a critical issue at several points in the quarter. Toward the end we were using a total of roughly 800 GB of disk space split between 5 sources, which made it hard to use efficiently. We also had some significant issues where the disk resources for virtual machines would (for one reason or another) be removed from the servers inventory. The students were mostly unable to reconnect to these virtual machines themselves with the result that they were unable to either free the disk space or reuse the virtual machines. Steve had partial access to address the problem, but it was often difficult to determine which files belonged to the class and which did not so he usually left it to the CSE staff to clean things up. Having more space in fewer sources and dedicated to the class would make it easier to both use it efficiently and to clean things up. It would also be nice if we could keep virtual machines from being removed from the inventory (either accidentally or through user action), though this may not be possible.

3. **Improved remote access.** We had 11 workstations dedicated for the students to use for remote access to the VMware environment. We had some problems where students would sometimes forget to logout, which would tie up one of the workstations until Steve could log them out by force. This might be improved by using some sort of inactivity logout on these machines. Remote access was also painfully slow for the Unix virtual machines.

4. **More VMware servers.** During project 2 we had a total of about 45 virtual machines running, and performance was noticeably affected. We got through everything OK, but it would be nice to have another VMware server available for running virtual machines on. This would certainly be required if we had more students in the course.

5. **Group Grading.** The students liked working in groups, and for the most part we think that the group project teams worked well. However, one of the groups consisted of a very knowledgeable and experienced student paired with 3 much less experienced students, and he ended up doing most of the work. This seemed like a potential problem - our grading scheme basically gives each student in a group the same grade, since most of the grade comes from the group papers and presentations. We would like to change the grading scheme somehow to allow us to differentiate grades within a group based on each member's contribution to the group effort.

D. Final Remarks

Overall, we felt that the course was a success. We want to teach it as a pilot course again in 2008. In the long term, we plan to make it as a project course, rather than a capstone one due to the nature of course projects and the popularity among graduate students.