B5 Lessons Learned From Teaching a Distance- Delivered Incident Response Course

J. Philip Craiger, PhD, University of Central Florida, Department of Engineering Technology, University of Central Florida, Orlando, FL 32816; Paul K. Burke, BS, Northeastern University, Boston, MA 02115; and Mark Pollitt, MS, University of Central Florida, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367*

The goals of this presentation are to: a) discuss the specific incident response knowledge and skills students are expected to demonstrate; b) compare and contrast the two modes of access, discussing advantages and disadvantages of both methods; and c) discuss a third method under investigation that involves virtualization software running on a server that is accessible over the internet.

This presentation will impact the forensic science community by providing educators and trainers with alternative methods of delivering hands-on, computer-based forensic projects and assignments that require a deal of realism.

Universities are increasing the number of online (distance) courses offered in order to reduce space requirements while allowing increased enrollment, both of which generate more revenue. Experience has taught us that there are courses that do not easily translate into an online format, particularly those that require students to complete hands-on assignments under quasi-realistic conditions in a physical computer lab. Over the last several years the authors have taught graduate and undergraduate versions of a course in Incident Response that requires students to assimilate concepts from the fields computer/network forensics and computer/network security. In this course students learn to identify and address factors related to computer incidents, such as: malware, hacker reconnaissance and exploits, insider access, social engineering, log file interpretation, and combining digital "evidence" to draw conclusions and make recommendations. The capstone project for this course requires students to manage a quasi-realistic 'live computer incident' where an external unauthorized user (hacker) has gained access to a 'privileged account' and attempts to control the server. Students must investigate the incident on a live, running server, which runs contrary to the "traditional" computer forensics process (pull-the-plug, create a forensic duplicate of the media, perform a forensic examination on the duplicate), but is a situation they may encounter under real- world circumstances.

This is a fairly simple assignment to create and manage provided it is run within a computer lab where a professor can supervise students as they are sitting at a computer terminal working on the problem. The same assignment run under an online class, however, creates issues for both professor and students, including: a) ensuring students can access

the server from a distance; b) ensuring students do not cheat; c) ensuring students have sufficient knowledge for the assignment, and; d) providing students sufficient access rights to conduct the investigation, while ensuring they cannot change or delete any important assignment or system files on the server.

Over the years two modes of student access to the 'victimized' server were used for the capstone assignment. In the first two class runs a Linux server was created that was 'self hacked,' leaving both obvious and non-obvious signs of unauthorized access and behavior. Each student was provided with an account, and students accessed the server over the Internet using SSH (a secure tunneling protocol). In the second two class runs virtualization software was used to create a Linux virtual machine that was again 'self hacked.' The running virtual machine was then 'suspended,' which wrote the state of the running system (i.e., contents of memory, running processes, etc.) to disk. The suspended virtual machine was compressed (zipped) and the compressed file uploaded to the course website. Students could then download the file, uncompress, and run it within the virtualization software running on their own computer.

Incident Response, Online Learning, Distance-Based Learning

 ** Presenting Author*