Student Information Security Lab Expansion

Proposer: Joseph N. Wilson
Associate Professor
CISE Department
Wertheim Engr. College
Rm E301 CSE Bldg. 42
Box 116120
Gainesville, FL 32611-6120
jnw@cise.ufl.edu
352-514-2191

Sponsoring Organization: Information Security and/or Infrastructure and Communications Technology

Purpose and Specific Objectives: **Impact/Benefit**:
I am requesting expansion of software licenses and equipment that currently supports about 180 students per year (and will be able to support up to twice as many due to expanded capacity). In short, tech fee funding will allow us to provide cybersecurity education and practical exercises to more students with better throughput and response time.

To understand the proposal fully, the evaluator must understand the concept of a computer virtual machine. For those not familiar with the concept, a virtual machine (VM) is a computer system that operates using emulation (simulation) on another computer. Most people are familiar with, for example, emulation of Gameboys or NES game systems on a Windows PC. You can take the software that one computer system (e.g. Gameboy) would use and run it on a different hardware platform (e.g. PC) using a program that simulates the behavior of the original computer. Modern computers provide hardware support for virtual machine emulation, allowing a single computer server to provide dozens of virtual computers networked together in various configurations. Access to these machines can be provided via internet connections that allow one to control the mouse and keyboard of the virtual computer as well as see what would be displayed on its monitor from a web browser or other remote console program. The user has the full experience of using a real, independent computer.

The purpose of this effort is to expand the CISE Department's existing capacity for providing networks of virtual machines to students for hands-on exercises that support information security education. The system employed to do this comprises hardware (5 Dell PowerEdge servers) and software, in the form of a Net Development Group (NDG) Virtual Environment system. The effort proposed here involves several different elements, namely, i) the acquisition of a software license that will let us double the number of virtual machine network pods (independent groups of VMs) that can be used for student activity and ii) the expansion of storage for supporting server equipment, enhancing our ability to provide the aforementioned networks of VMs. In our proposal concept paper, we discussed possible purchase of network switches to support this hardware configuration. Since the proposal concept paper was submitted, we have found a donor who will provide network switches compatible with our systems to support our effort. This donor will also loan other supportive equipment. In this expanded hardware setting, we realized that expanded disk storage is necessary to support the final configuration of machines and are requesting that in this proposal. The net reduction in our funding request totals $13,003.

The reason this facility is so important is that the networks of virtual machines we provide to students allow us to deploy systems that are disconnected from the internet and allow us to use software that would normally be considered unsafe on a typical university network. All year long, the system is used to provide special security exercises to members of the UF Student Information Security Team and is used to help the Collegiate Cyber Defense Competition (CCDC) team learn how to defend and secure computers and networks. Every spring, the system supports the offering of a malware reverse engineering class. The networks contain actual malware such as ransomware, banking Trojans, and rootkits, that would (or should) be barred from use on a university network. Having our NDG system lets us deploy that with no danger of subsequent infection. Every fall, the system supports

the teaching of a penetration testing class in which students learn offensive security techniques (ways to exploit vulnerabilities in poorly configured machines and networks) as well as defenses against such vulnerabilities. Many of the techniques taught to those students require the use of tools that are banned by the university network, and accidental misuse of them can result in significant negative outcomes. Once again, the use of the NDG system lets us insure that students are only able to apply these tools to machines that are within the scope of their investigations.

To help the evaluation committee appreciate the role this system plays in an understandable way, I'll describe several scenarios of the use of this network that have occurred just in the past few weeks and also describe the fall class activities in more detail.

In the UF Student Infosec Team's meeting of Thursday 22 March they introduced the concept of reverse engineering to their newer members with hands-on exercises carried out in 231 CSE Computer Lab, maintained by Academic Technology. To prepare for this meeting, the students configured a virtual machine that contained the appropriate software necessary for students to individually analyze, understand, and possibly modify an executable program for which they do not have the source code. In order for each student to be able to understand the problem this VM was replicated and 32 copies (the maximum allowed by our current software license) were provided for simultaneous access. This meeting was attended by 47 students, meaning that at least 30 students were doubled-up on a single VM. While these VMs can be provided to students to run on their own machines, there are numerous problems that can arise during VM installation and emulation that can be difficult to debug in the context of a meeting with dozens of people in which you're actually trying to teach people something interesting and complex. Being able to rely on the VMs just working significantly aids in helping people understand the processes and types of thinking that go into such information security activities. More than 90 students attended each of the first three meetings of the club. Being able to provide service for 64 students will enhance our ability to serve more students better in this organization.

In the *Malware Reverse Engineering* class during the last few weeks, 24 students have been provided access to Windows virtual machines that have actual malware samples contained on them. This semester, the students have analyzed the behavior of the Hermes 2 ransomware which was used as part of a Taiwan bank heist in 2017. They've also used these systems to investigate the behavior of a malware artifact known as Evil Pony which is used as a banking Trojan. It captures username and password credentials from a wide variety of applications and exports them to a command and control server. Running these programs on a machine that is actually connected to the internet can be dangerous at best and disastrous at worst. By using the NDG system, students can avoid risking infection of their own personal machines and can engage in more thorough investigations as a result of being freed from the worry of what might happen if they accidentally run these programs in an unsafe way.
At the 24 March meeting of the Collegiate Cyber Defense Competition (CCDC) team, the 9 students who will represent UF at the Southeast Regional Competition on April 2 and 3, met together to practice for their competition. They used a network of 17 virtual machines that was designed to closely match the computer network they will be using during competition. Their job is to maintain a variety of services (web, email, databases, e-commerce, firewalls, domain name service, and others) on a collection of computers running various operating systems and software packages. While they were doing this, a group of red teamers (offensive security specialists) were attempting to break into their machines (which had vulnerabilities resulting from software versions and configuration errors) and interfere with the functioning of the system. It's the team's job to keep the services running, remove the vulnerabilities that the red teamers are exploiting, prevent further intrusion, and carry out tasks as assigned by their business division. This kind of experience is impossible to achieve if actual hardware resources must be used to implement the desired configuration because of the wide variety of systems that might be encountered in practice, not to mention the hardware configuration issues. Furthermore, configuring these systems using real hardware is much more time consuming and difficult that deploying them with VMs.

In the fall of 2017, 61 students in the *Penetration Testing—Ethical Hacking* class worked all semester long on a series of laboratory exercises that involved networks of VMs that represented the computer network of M3g4c0rp, a fictitious business that engaged them to be penetration testers. M3g4c0rp's network contained two routers, one outward facing web server, a Windows server and a Linux development server, as well as three PCs. In addition to

this, each student had a VM running Kali Linux—a Linux distribution designed for penetration testers. They engaged in over 20 different labs aimed at identifying and exploiting vulnerable software and configurations as well as learning how to avoid these vulnerabilities. One of the exploits they used in order to gain unauthorized access to a Windows server was Eternal Romance, an exploit made available in the recent Shadow Brokers release of tools developed and used by the NSA. Penetration testers are engaged by companies specifically to attempt to gain unauthorized access to systems and try to access protected data so that companies can identify insecure software and configurations. They are paid to do what would be illegal to do otherwise. Similarly, students cannot engage in these activities on any real systems available anywhere on campus or elsewhere due to possibility of causing unintended harm to other systems not being intentionally targeted. They can, however, carry out these activities on VMs that are disconnected from the internet without worrying that they might accidentally break into a system that is "out of scope," as so often happens to actual penetration testers. (They all have stories about this.) Expanding our system will allow more students to have more time to carry out such exercises in the future.
I hope these examples have given the evaluation committee a sense of the important role this system plays in cybersecurity education at the University of Florida.

In a previous Technology Fee Proposal (Virtual Environment for Information Security Education and Exploration – 2013), we were awarded $25,910 to support acquisition of hardware and software to provide information security education to UF students in class and in conjunction with the UF Student Information Security Team, a UF club. We used those funds, together with other resources totaling $48,352 to provide the hardware/software environment we currently have in place and have been supporting for five years. We will be improving that system. We have used it to provide classroom support for over 80 students per academic year in UF courses and all students in the UF Student Infosec Team (over 100 individual students this academic year). Ongoing support contracts have totaled approximately $15,000 over this time period. The technology fee grant program's investment of less than $100 per classroom student (half that if you consider UF-SIT students) helped leverage a project with a total investment of roughly 2.5 times that magnitude.

Current software constraints allow us to support only 32 simultaneous users of this system. We are requesting funds to allow us to double this number through the expansion of our systems Netlab Virtual Edition to a 64-user license. We have the hardware necessary to support this modification. The software license fee for 32 extra users costs $19,900 with a $2,995 support license.
One issue associated with supporting 64 users on this system is the effective use of the supporting hardware. We will be able to achieve better performance with the addition hardware switches being donated to us. These switches will connect the 5 networked computers currently supporting this effort into a single cluster that supports dynamic load balancing. These systems are maintained in our CISE Departmental server room and are managed by CISE staff and faculty. Students only have physical access to these machines under direct supervision of faculty or staff. In addition to the donation of these switches, we will be receiving a two-year loan of three more Dell PowerEdge servers to support our UF-SIT and CCDC efforts. These will be housed in our Department's selfmanaged server room which allows physical access to approved students and faculty. This will provide several

benefits, namely, i) the CCDC team can experiment with a variety of hardware devices—such as specific switches and other network gear—that do not have effective VM emulation software, ii) the Student Infosec Team will be able to get access to this gear over the network to support the organization's activities even when the primary VM system is fully booked due to classroom usage, and iii) students will get an opportunity to use the VMware ESX operating system that implements the hypervisor system, something they cannot do with our current departmental system because of the need for reliability and availability: we can't let students experiment on that system, only on the VMs it runs. To support these extra machines, we are requesting 6 6TB drives (2 for each server) at a cost of $950, a network attached storage (NAS) system ($427), and disks for the NAS ($920).
Our request amounts to $25,192 in total.

Sustainability:
Continuing maintenance, support, and configuration will be provided by the CISE Department's IT staff together with faculty, as well as graduate and undergraduate students, who provide educational materials in the form of education exercises that employ the virtual machine networks supported by this project. Our track record of

supporting the resources we purchased with support from our previous Tech Fee grant demonstrates our dedication to this task. In addition, the support we are receiving from outside the university through donations also shows that this is a task that brings together a wide variety of people all working together to provide a better environment for cybersecurity education and training.

Timeline:
Implementation of the plan outlined above will take place as soon as funds are received. Software licenses, subject to the usual purchasing delays, should be in place within 2 months of award. The small amount of requested hardware can be acquired within a matter of days of approval. CISE IT staff can install all new hardware elements during the regular course of business and the upgraded system should be operational well within 3 months of the award date.

Budget:
NETLAB+ Virtual Edition with 32 (extra) active pods $19,900
NETLAB+ VE Support for 1 year $2,995
Server disk storage expansion (6 @ 2.5in 6TB hard drive) $950
Network Attached Storage server (Synology DS418 NAS device) $427
Network Attached Storage disks (4 @ 3.5in 6TB hard drive) $920

Total $25,192