HANDS-ON COMPUTER SECURITY WITH A RASPBERRY PI *

Adam H. Villa
Department of Mathematics and Computer Science
Providence College
Providence, RI 02918
401 865-2132
avilla@providence.edu

ABSTRACT

Computer security is a popular topic in today's world, whether it appears in the form of a newspaper headline or a job posting. The need for students to have hands-on experience with computer security topics and software is paramount. Employers are increasingly interested in hiring students with security knowledge, especially those familiar with popular security software packages and low-level security tools. This paper details the use of a small, portable computer called a Raspberry Pi for instructing real-world computer security concepts via hands-on laboratory assignments. The benefits of using these small computers in lieu of a dedicated computer lab include: decreased expenses, isolated sandbox environments, greater flexibility in designing assignments, and utilizing existing classroom spaces.

INTRODUCTION

Interest in computer security has grown dramatically in the past decade. This increased interest has been motivated by many factors including continual security breaches, identity theft, and popular denial of service attacks. Students' interest has subsequently been piqued by the topic and the number of jobs in the security field has promoted additional interest in the field.

In addition to student interest, there has been a push for in the inclusion of computer security topics in computer science programs across the country. Information Assurance and Security (IAS) is now a key knowledge area that was added to the most recent iteration of the Computer Science Curricula study conducted by the Joint Task Force on

---

Computing Curricula of the Association for Computing Machinery (ACM) and the IEEE Computer Society in 2013 [14]. The task force's motivation for this topic's inclusion in the main knowledge areas is in "recognition of the world's critical reliance on information technology and computing".

There have been many recent studies and papers that examine techniques and approaches for teaching computer security. Several studies examine how to integrate computer security topics into existing courses [10, 11, 20, 21]. Researchers have identified specific applications and tools that are useful for teaching computer security classes [6, 9, 17, 19] There has also been much work done to develop labs, activities, and exercises for computer security courses [1, 2, 3, 5, 7, 8, 12, 13, 15, 16, 18, 22, 23, 24]. Many of these labs however are designed for dedicated computer lab spaces or dedicated computer networks or even virtual machine environments.

The troubling aspect of many computer security hands-on activities or lab assignments, especially ones that explore malicious activity, is the impact that they could possibly have on campus users and on system resources. By using completely separate hardware and networking devices, we can ensure that the work conducted by the students will not impact other people and their workloads. In lieu of creating a dedicated computer lab or using virtual environments, utilizing Raspberry Pi computers is a perfect solution. These small computers are easy to setup and connect to existing peripherals. Students can even take them home to work on projects and assignments outside of class meetings.

The hands-on lab assignments described in this paper can be conducted on Raspberry Pi machines using an existing computer lab on campus. A completely separate and private network can be created using wired or wireless connections. The following section details several possible lab assignments that worked well with the Raspberry Pi computers. The labs were designed for upper-level students that have had some exposure to both operating systems and networking concepts.

LAB ASSIGNMENTS USING THE RASPBERRY PI

All lab assignments are conducted during class meeting times where the instructor and possible assistants are available for guidance and troubleshooting assistance. Depending on the number of students and the number of Raspberry Pi computers used for the labs, the size and setup of the private network used by the devices can vary. Figure

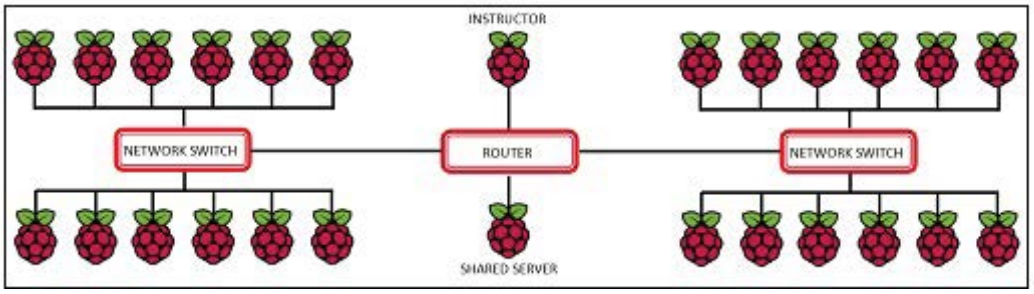

Figure 1: Possible lab configuration using the Raspberry Pi computers and private network components

1 illustrates a possible setup with 26 Raspberry Pi computers: 24 student machines, 1 instructor machine, and a shared server that are connected using two switches and one router. The two switches and the instructor machine are connected to the router and all students connect to a specific switch based on their physical proximity in the room.

The next sections describe five lab assignments that could be conducted using the Raspberry Pi computers and the private network. These lab assignments are by no means exhaustive and could easily be augmented or reduced based on course objectives and allotted time. The labs presented were well received by the students and were effective at reinforcing core security concepts.

Lab #1 - Network configuration, firewall configuration

Using the Raspberry Pi computers and the Raspbian OS, the students can gain firsthand knowledge on how to use software level firewalls and configure network connections. Many students are familiar with Windows or MacOS network configuration tools and their built-in firewalls, however Linux based variants are often foreign to them. Since the Raspberry Pi computers are not as intimidating to most students and the fact that the entire OS can be reset to factory defaults quickly, the students have very little trepidation when it comes to configuring the operating system and networking components.

In the lab, students are given the task to configure the iptables firewall rules for the system. During the lab the students are asked to disable certain types of network traffic and various network ports. In the written lab report, students are required to discuss the positive and negative impacts of blocking specific traffic classes and ports.

Lab #2 - Network traffic monitoring

This lab requires students to install and setup various services on the Raspberry Pi computers, such as a web server, FTP server, and MySQL server. Once these services are setup, students utilize multiple applications to examine network traffic and open ports on each other's machines. The purpose of this lab is to familiarize the students with the traffic analysis tools currently available and to drive home the idea that certain pieces of information are available to people on the shared network.

Since the network used by the Raspberry Pi computers is private, there is no risk of accidently examining live, sensitive data on the campus network. Students should be instructed to never send confidential information/data while working on the Raspberry Pi labs. All data transmitted/stored should be viewed as publicly accessible. The tools used by the students include: TCPDUMP, iptraf, and nmap. Figure 2 illustrates a summary table that the application can produce.

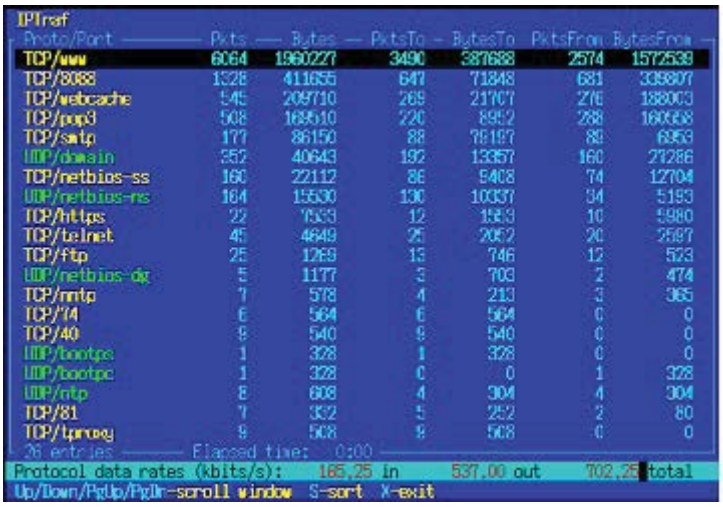

Figure 2: Sample iptraf application output after examining network traffic.

Lab #3 - Denial of Service Attacks

This popular lab allows the students to try various Denial of Service attacks. This lab benefits the most from using Raspberry Pi computers on a private network. The students can try multiple attack vectors without concern for other users on the campus network, since they are completely isolated. There is also no risk of damaging network configurations or operating systems since everything can easily be reset.

The students implement and examine three types of DoS attacks: Ping Attacks, TCP SYN Attacks, and UDP Flood Attacks. For each attack, students are asked to create a report that details the setup of the attack, why the attack renders the victim inaccessible, and how the victim can recover from the attack. Before the attack begins the class selects a victim that will receive the flood of network traffic. The victim prepares for the oncoming attack by monitoring network connection traffic and logging the number of requests on a particular service. At a designated time, the remaining members of the class conduct the DoS attack. The class examines the victim's machine and makes observations about various performance metrics. The class would then stop the attack and discuss a possible solution to prevent it from happening again. The victim would implement the decided upon procedure and the attack would re-commence. The class would continue to monitor the performance metrics of the victim's machine.

Lab #4 - Examination of existing OS and find problems/fix problems

Prior to the lab, a testing Raspbian OS environment is created. In this environment, various OS settings and other items are improperly or insecurely configured. The specific items can be modified to meet the goals of the course. For example, the firewall could be improperly configured or user authentication could be handled incorrectly. Once the insecure OS is created, it can be copied to a spare set of SD memory cards. Students are then provided with the card at the start of the lab. The students are asked to treat the Raspberry Pi and its operating system as a specific type of a machine, for example a web server, a database server, or a file server. It is their task to examine the operating system, applications, users, and services to identify issues. A lab report is created that describes

their findings and their proposed solutions to rectify those problems.

This lab could be run multiple times with different operating system configurations. During the different iterations of the lab, the type of machine emulated by the Raspberry Pi could also vary. For example, instead of a web server, the students could be presented with an image that represents a MySQL database server.

Lab #5 - Encryption and Cryptography

In this lab students are asked to examine existing tools for secure data communication. After thoroughly studying the concepts behind cryptography and encryption standards, students will be able to use real world applications that utilize the concepts that have been studied. The lab utilizes the cryptography library built into the OpenSSL application. The lab requires that the instructor create a shared storage space on the private network. This could be the instructor's Raspberry Pi or a spare device. This shared storage will be used for message passing between students and a centralized key repository.

The students begin the lab by creating public and private RSA keys using the OpenSSL application. They keep their private keys on their own machine (in a secure location) and copy their public key to the central key repository folder on the shared machine. After the students are comfortable with the OpenSSL application, they will then use the application to create a message digest for a simple file. Students can explore the variety of message digest formats supported by OpenSSL, which include sha1 and md5. The students create a message digest for a text file that is subsequently signed using their private key. They upload both their text file and their signed message digest to a directory on a shared machine. Students will download a classmate's file and the associated message digest file to their own machines. Using OpenSSL, they will verify that the specified author is valid using the author's public key and they will verify that the file has not been modified since it was signed by the author. Prior to this step, the instructor could modify one or more data files in the shared directory or produce a message digest using a different key. This would allow the students to see what would happen if a message was modified after the md5 value is created or signed by a different person.

Another component of this lab challenges the students to communicate securely with each other. The students must encrypt a data file using symmetric encryption and then subsequently share the key used for the symmetric encryption with another person in the class using separate public/private key encryption. This part of the lab allows the student explore different encryption techniques and identify the challenges of working with multiple keys.

OUTCOMES AND FUTURE WORK

The lab assignments presented in this paper and the use of the Raspberry Pi computers were very well received by the students. The students were excited to use the Raspberry Pi devices on lab days. On the course evaluations, the number one positive item indicated by every student in the course was the use of the Raspberry Pi computers.

Due to their small form factor and the use of an easily replaceable SD memory card, the students were not intimidated by the machines. Students that were originally reluctant to try commands on a shared course server were uninhibited when they used these small computers. From a purely logistical standpoint, setting up and tearing down the lab environment in a computer classroom took at most ten minutes, which was ideal due to the fact the classrooms on campus are heavily utilized by all departments throughout the day.

Students continually requested for more class time to be dedicated to the Raspberry Pi devices and their associated lab assignments. This has motivated the design of additional labs and activities to be incorporated into the course. It has also potentially motivated a flipped classroom approach to the course for future semesters.

REFERENCES

[1] Aman, J., Conway, J., and Harr, C., A capstone exercise for a cybersecurity course. *J. Comput. Sci. Coll*, 25, (5), 207-212, 2010.

[2] Aman, J, Black Hat/White Hat: an aggressive approach to the graduate computer security course, *J. Comput. Sci. Coll*, 22, (2), 52-58, 2006.

[3] Bailey, M., Coleman, C., and Davidson, J., Defense against the dark arts. *Proceedings of SIGCSE*, 315-319, 2008.

[4] Ben Othmane, L., Bhuse, V., Lilien, L.T., Incorporating lab experience into computer security courses, *Proceedings of WCCIT*, 1-4, 2013.

[5] Brustoloni, J., Laboratory experiments for network security instruction, *J. Educ. Resour. Comput.*, 6, (4), Article 5, 2006.

[6] Dangler, J. and Barrett, M., Security teaching modules for computer science courses. *J. Comput. Sci. Coll*, 29, (2), 178-183, 2013.

[7] Du, W., and Wang, R., SEED: A Suite of Instructional Laboratories for Computer Security Education, *J. Educ. Resour. Comput*., 8, (1), Article 3, 2008.

[8] Frank, C., Mason, S., Micco, M., Montante, R., and Rossman, H., Panel discussion: laboratories for a computer security course, *J. Comput. Sci. Coll*, 18, (3), 2003.

[9] Frank, C. and Wells, G., Laboratory exercises for a computer security course, J. Comput. Sci. Coll, 17, (4), 51-54, 2002.

[10] George, B., Klems, M., and Valeva, A., A method for incorporating usable security into computer security courses, *Proceedings of SIGCSE*, 681-686, 2013.

[11] Herath, J., Herath, S., and Herath, A., Integration of computer security laboratories into computer architecture courses to enhance undergraduate education. *Proceedings of WCAE*, Article 7, 2003.

[12] Holland-Minkley, A., Cyberattacks: a lab-based introduction to computer security, *Proceedings of SIGITE*, 39-46, 2006.

[13] Huss, J., Laboratory projects for promoting hands-on learning in a computer security course, *SIGCSE Bulletin*, 27, (2), 2-6, 1995.

[14] Joint Task Force on Computing Curricula - Association for Computing Machinery (ACM) and IEEE Computer Society. 2013. Computer Science Curricula 2013, Curriculum Guidelines for Undergraduate Degree Programs in Computer Science.

[15] Kazemi, N. and Azadegan, S., IPsecLite: a tool for teaching security concepts, *Proceedings of SIGCSE*, 138-142, 2010.

[16] LeBlanc, C., and Stiller, E., Teaching computer security at a small college, *Proceedings of SIGCSE*, 407-411, 2004.

[17] Lawrence-Fowler, W.A., A Computer Science course in Cyber Security and Forensics for a multidisciplinary audience, *Proceedings of the Frontiers in Education Conference*, IEEE , 1971-1976, 2013.

[18] O'Leary, M., A laboratory based capstone course in computer security for undergraduates, *Proceedings of SIGCSE*, 2-6, 2006.

[19] Riabov, V., and Higgs, B., Running a computer security course: challenges, tools, and projects: poster session, *J. Comput. Sci. Coll*, 25, (6), 245-247, 2010.

[20] Siraj, A., Ghafoor, S., Tower, J., and Haynes, A., Empowering faculty to embed security topics into computer science courses, *Proceedings ITiCSE*, 99-104, 2014.

[21] Tang, C., Hawthorne, E., Taylor, B., and Kaza, S., Introducing security and responsible coding into introductory computer science courses, *J. Comput. Sci. Coll*, 29, (1), 148-149, 2013.

[22] Trabelsi, Z., and Alketbi, L., Using network packet generators and snort rules for teaching denial of service attacks, *Proceedings of ITiCSE*, 285-290, 2013.

[23] Wagner, P., and Wudi, J., Designing and implementing a cyberwar laboratory exercise for a computer security course, *Proceedings of SIGCSE*, 402-406, 2004.

[24] Wulf, T., Implementing a minimal lab for an undergraduate network security course, *J. Comput. Sci. Coll*, 19, (1), 94-98, 2003.