8-13-2019

To equip tomorrow's cybersecurity experts, we'll need an open approach

Brandon Dixon
Murray State University, bdixon2@murraystate.edu

Randall Joyce
Murray State University, rjoyce@murraystate.edu

To equip tomorrow's cybersecurity experts, we'll need an open approach

An open approach to training the next generation of cybersecurity experts can fully equip them to combat a constantly shifting threat landscape.

Brandon Dixon & Randall Joyce, 13 Aug 2019

Today's world—marked by an increase of Internet-connected devices, digital assets, and information systems infrastructure—demands more cybersecurity professionals. Cybersecurity is the practice of defending these devices, assets, and systems against malicious cyberattacks from both internal and external entities. Often these cyberattacks are linked to cybercrimes, or crimes committed using a computer to generate profit or to affect the integrity, availability, and confidentiality of the data or system. In 2016, cybercrimes cost the global economy more than $450 billion.

Developing a robust cybersecurity workforce is therefore essential for mitigating the effects of cybercrime on the global economy. The United States Bureau of Labor Statistics has predicted a shortage of 1.8 million cybersecurity professionals by the year 2022. The United States has already developed a working group, the National Initiative for Cybersecurity Education (NICE), to promote cybersecurity education. Educators play a critical role helping promote cybersecurity as early as possible in academic organizations. And they should take an open approach to doing it.

It's critical for students to not only become acquainted with the advantages of open source software but also to develop strong skills working openly, since open source software is not only common in the IT industry in general, but is specifically necessary in the field of cybersecurity. With this approach, students can learn within the safety and guidance of the classroom while also naturally acquiring research and troubleshooting skills by facing challenges that are presented or arise during exercises.

In this article, we'll explain how experiencing these challenges in the classroom environment is imperative for preparing students for the industry and equipping them to face the unforgiving challenges that await them in the IT industry—especially in the rapidly evolving cybersecurity field.

Developing an open approach to cybersecurity education

Open source software, open source communities, and open source principles have been pivotal in the adoption of computer automation that is so common today. For instance, most smart devices are running a version of the Linux kernel. In the cybersecurity field, it's common to find Linux at the heart of most operating systems that are running on security appliances. But going beyond the operating system, Ansible has taken the management scene by storm, allowing for simplified automation of management tasks that even professionals without programming or scripting experience can quickly grasp and begin to implement. In addition to the benefits of automation, a variety of open source applications provide seemingly limitless capabilities for computer users—such as the ability to create video, music, games, or graphic designs on par with proprietary software. Open source software has often been the creative spark that has enabled countless individuals to pursue goals that would have otherwise been unobtainable.

Open source has had the same democratizing effect for cybersecurity professionals. Like other open source projects, open source cybersecurity tools receive extensive community support, so they're often some of the most-used security tools in existence today. Such tools include Nmap, OpenVAS, OSSEC, Metasploit Framework, Wireshark, and the Kali Linux distribution, to name a few. These open source tools are an invaluable asset for educators, as they provide an opportunity for students to use the same cybersecurity tools currently being used in industry—but within a safe learning environment, a factor that is critical for student growth in the field.

In Murray State University's Telecommunications Systems Management (TSM) program, we're developing curricula and resources aimed at getting students excited about cybersecurity and motivated to pursue it. But students often enter the program with little or no understanding of open source principles or software, so bringing participants up to speed has been one of our biggest challenges. That's why we've partnered with Red Hat Academy to supplement our materials and instill fundamental Linux skills and knowledge into our students. This foundation not only prepares students to use the open source security tools that are based on Linux operating systems but also equips them to experiment with a wider variety of Linux-based open source cybersecurity tools, giving them valuable, hands-on experience. And since these tools are freely available, they can continue practicing their skills outside the classroom.

Equipping students for a collaborative industry

As we've said, open source software's ubiquity and ample community support makes it critical to the field of cybersecurity. In the TSM program, our courses incorporate open tools and open practices to simulate the environments students should expect to find if they choose to enter the cybersecurity industry. By creating this type of learning experience in the classroom—a place where instructors can offer immediate guidance and the stakes are low—we're able to help students can gain the critical thinking skills needed for the variety of challenges they'll encounter in the field.

Chief among these, for example, are the skills associated with seeking, assessing, understanding resources from cybersecurity communities. In our courses, we emphasize the process of researching community forums and reading software documentation. Because no one could ever hope to prepare students for every situation they might encounter in the field, we help students *train themselves* how to use the tools at their disposal to resolve different situations that may arise. Because open source cybersecurity tools often give rise to engaged and supportive communities, students have the opportunity to develop troubleshooting skills when they encounter challenges by discovering solutions in conversation with people outside the classroom. Developing the ability to quickly and efficiently research problems and solutions is critical for a cybersecurity student, since technology (and the threat landscape) is always evolving.

A more authentic operating system experience

Most operating systems courses take a narrow approach focused on proprietary software, which is an injustice to students as it denies them access to the diversity of the operating systems found in the IT industry. For instance, as companies are moving their services to the cloud, they are increasingly running on open source, Linux-based operating systems. Additionally, since open source software enables developers to repackage the software and customize distributions, many are adopting these varying distributions of Linux simply because they are a better fit for a particular application. Still others are moving their servers from proprietary platforms to Linux due to the attraction of the accountability that comes with open source software—especially in light of frustrations that occur when proprietary vendors push updates that cause major issues in their infrastructure.

In the TSM courses, our students gain a strong understanding of foundational Linux concepts. In particular, the curricula from Red Hat Academy gives students granular experience with many of the foundational commands, and it allows them to gain an understanding of a popular open source system design. Linux has a well-developed community of other users, developers, and tinkerers that provide an excellent forum for students to engage other open source users for help. Having students develop a strong foundational knowledge in Linux is critical as they progress through the TSM program. As students work through their courses, they naturally develop their knowledge and skills, and by obtaining this hand-on experience they also gain a foundation that prepares the student for a variety of careers—becoming traditional security analysts, for example, or pursuing careers in penetration testing using Kali Linux. No matter their path, having a strong Linux background is essential for students.

Embracing community-driven development

One of the major frustrations in the IT field is being forced to use tools that simply do not work or quickly become unusable. Often, software purchased to accomplish some particular task will quickly become obsolete as the vendor offers "upgrades" and "add-ons" to accommodate the changing needs of their customer—at a price. This experience isn't limited to IT experts; end users also experience this frustration. Driving this practice this is, naturally, a desire to maintain long-term profits, as companies must continue to sell software to survive or must lock their users into subscription models.

The fact that much of the open source software in use today is provided free of charge is enough to draw industry experts to use it. However, open source software is more than just freeware. Because the users of those tools have formed such large communities, they receive proportional support from their communities as well. It's not unusual to see small projects grow into full software suites as users submit feedback to community driven development. This type of feedback often creates products that are superior to their paid counterparts, which do not have such a direct line into the community they seek to serve. This is absolutely true in the case of cybersecurity tools, where the majority of the most popular tools are all open source, community-driven projects. In the TSM program, students are well-versed in tools such as these, thanks to the availability and free distribution model that open source software affords. The result is that through hands-on use, students gain a firm understanding of how to utilize these types of tools.

Future proofing

Staying relevant in the IT industry is a constant battle, especially when dealing with the many products and solutions that are always seeking to gain market share. This battle extends as well to the "soldiers on the ground," who may find keeping a diversified toolset difficult when many of the solutions are kept out of their hands due to a price ceiling.

Open source software provides students, who come from a variety of socio-economic backgrounds, with the opportunity to expand their experience without needing to be employed in a particular field, as the software is readily available to them through open source distribution channels. Similarly, graduates who find jobs in one particular segment of the market still have the opportunity to train their skills in *other* areas in which they may be interested, thanks to the breadth of open source software commonly used in the IT industry.

As we train these students how to train themselves, expose them to the variety of tools at their disposal, and educate them on how widely used these tools are, the students are not only equipped to enter the workforce, but are also empowered to stay ahead of the game as well.