ISSN: 2473-3857
v3 n4380

Cyber Defense Education & A Linux Toolkit

Jennifer Wescott
jar2569@uncw.edu

Dr. Ulku Clark
clarku@uncw.edu

Information Systems
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

As cyber-criminals continue to increase their skills and threaten organizations and individuals worldwide, we take a look at the growing gap between cyber security jobs versus the available human capital, we review cyber security education, the current curricula framework and where the Linux Operating System falls within that framework. Briefly presented is the Linux Toolkit that has been created to aid in teaching students skills they can continue to build as they go into a career in cyber security.

Keywords: cyber security, curricula, linux, education

1. INTRODUCTION

It is more important than ever to get students involved in Science, Technology, Engineering, and Math (STEM) education and have them go on to corresponding careers. More pressing though is the sector that employs the vast field of cyber security. The need for cyber security professionals is growing each day, and we have seen this more over the last several years with Anthem Blue Cross and Blue Shield where around 80 million people were affected (McGee, 2017), Target had around 40 million debit/credit cards stolen (Krebs, 2014), Yahoo totaled around 3 billion accounts accessed (Burgess, 2017), and the latest ransomwares including WannaCry which crippled services within hospitals and other facilities in the United Kingdom , and NotPetya which hindered Ukrainian infrastructure such as the power grid, airports, and public transit (Newman, 2017).

This paper is going to focus on the importance of cyber security, the current curriculum, and the Linux Toolkit that will be implemented to help beginner students become not only knowledgeable in Linux and virtual machines but also become more interested in the security field in general.

2. LITERATURE REVIEW

The State of Cyber Security

Over the past several years, there have been statements by officials like the Defense Secretary, FBI Director, and Director of National Intelligence who have all stated the importance of cyber security within national security and defense. It is "as important a military domain as land, sea, air, and space," stated by William Lynn, the 2010 US Deputy Defense Secretary (Vogel, 2016, p. 33). Cyber attacks have the potential to devastate areas in our lives such as our health, wellness, power/energy, food, water, and our general safety (Spidalieri & Kern, 2014). These are everyday items that we are accustomed to, and to lose them for "x" amount of days, weeks,

©2017 ISCAP (Information Systems & Computing Academic Professionals)

ISSN: 2473-3857
v3 n4380

or even months due to a cyber attack could cause massive disarray.

There is currently a trend in reliance on utilizing the latest security tools and technology when preventing and/or detecting cyber threats. Unfortunately, tools and technology alone will not suffice when it comes to cyber security. There needs to be more of a focus on people, and those people need to be effectively developing, implementing, and/or maintaining those security tools and technology (Spidalieri & Kern, 2014).

Cyber Security Employment Supply & Demand and Educational Opportunity

The growing number of jobs needing to be filled within the cyber security workforce is nothing new, and as stated in the 2017 Cybersecurity Curricula, "Findings from the International Information Systems Security Certification Consortium (ISC)^2 workforce survey predict that by 2020 there will be a global shortage of 1.5 Million cybersecurity professionals," (Burley, D. L. (JTF Co-Chair et al., 2017; NICE, p. 58). And in 2014, 64% of high school students did not even have access to classes that would put them on a path for a career in cyber security (Vogel, 2016). Looking at these numbers, the lack of curricula, and the gap in the pathway to a cyber security career is evident.

While we are trying to figure out what to do about these problems, the black hat, offensive hackers are continuously gaining more skills. Vogel (2016) sums it up by saying that the speed at which the offensive cyber-criminals are committing their crimes is surpassing the defensive "human capital" that is employed. This is the reason there is such a need and a feeling of immediacy to implement/expand the education and training in cyber security (Vogel, 2016).

There is a large window here for students to learn and gain the needed security skills for employment. As the demand for human capital increases, the opportunities surge for up-and-coming students to pursue a certain field in cyber security (Vogel, 2016). Students can essentially start learning niche, specialized areas such as social media exploitation, forensic computing, or threat intelligence reporting - making it easier for them to stand out (Vogel, 2016).

While the time is right for universities to embrace cyber security, there continues to be a "fog" over the industry in that there needs to be a framework of sorts created to then develop, manage, and oversee the training and continued education of a suitable cyber security workforce (Spidalieri & Kern, 2014). According to Burley et al. (2017, p. 66), "roadmaps represent the ideal plan of study", but implementing roadmaps within a university setting can be very difficult. Even with obstacles, this education is obviously and necessarily needed to ensure the cyber security employment gap does not continue to widen.

Lacking Programs and Recent Curriculum Model

Spidalieri & Kern (2014) report that few American educational institutions offer programs that combine cyber security and other disciplines. Even fewer encourage cross-departmental collaboration, which is necessary when various disciplines such as technology, policy, and business fall under the cyber security umbrella.

In fact, during an interview with Melissa Hathaway, who spearheaded the Cyberspace Policy Review for President Barack Obama and is leading the Comprehensive National Cybersecurity Initiative (CNCI) stated, "The problem is that we are not even teaching the basics of computer security in schools and university programs in general, and that cybersecurity is still not part of most computer science departments and other university departments' core curricula... We will never get to the workforce needed until we have the majority of schools and universities teaching the basic skill sets required in the field and this becomes part of a standardized core curriculum, just like basic history, math, and other basic courses. Cybersecurity, after all, is part of everyday life!" (Spidalieri & Kern, 2014, p. 8).

To answer this need, in 2015, the Association for Computing Machinery (ACM) Education Board assembled what is now known as the Joint Task Force on Cybersecurity Education (CSEC2017). This Education Board and Joint Task Force (JTF) is comprised of professional and scientific computing groups and/or societies such as the ACM, Institute of Electrical and Electronics Engineers Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) (Burley, D. L. (JTF Co-Chair et al., 2017).

CSEC2017 describes cyber security as still being in the beginning stages and the JTF has put together some information to help guide the curriculum starting with the characteristics of a

©2017 ISCAP (Information Systems & Computing Academic Professionals)

ISSN: 2473-3857
v3 n4380

cyber security program. The framework content needs to be both on 1) learning and understanding concepts and theory as well as 2) opportunities for students to gain practical skills through application of that knowledge (Burley, D. L. (JTF Co-Chair et al., 2017)).

Based on reviews of science, computing, and cybersecurity educational curricula, a thought model was created and refers to the following four dimensions: 1) knowledge areas, 2) cross-cutting concepts, 3) disciplinary lens, and 4) application areas. And while not named as one of the dimensions, "foundational knowledge" is considered the blue area underlying the knowledge areas and cross-cutting concepts depicted in *Figure 1* (Burley, D. L. (JTF Co-Chair et al., 2017).

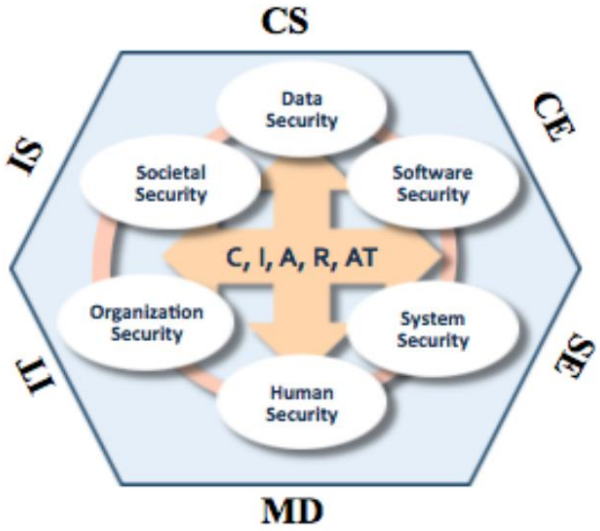

Figure 1 – This figure displays the framework for which institutions can begin to implement and focus on certain areas within cyber security Burley, D. L. (JTF Co-Chair et al., 2017, p. 18).

Depicted in *Figure 1,* the six *knowledge areas* in the CSEC2017 thought model represent the "full body of knowledge within the field of cybersecurity" and include: 1) data security, 2) software security, 3) system security, 4) human security, 5) organizational security, and 6) societal security. (Burley, D. L. (JTF Co-Chair et al., 2017, p. 18).

The *disciplinary lens* represents disciplines that form the foundation of a cybersecurity program which consists of the following five computing disciplines: 1) computer science (CS), 2) computer engineering (CE), 3) information systems (IS), 4) information technology (IT), 5) software engineering (SE), and 6) mixed discipline (MD). (Burley, D. L. (JTF Co-Chair et al., 2017).
Finally, the five *cross-cutting concepts* are 1) Confidentiality (C), 2) Integrity (I), 3) Availability (A), 4) Risk (R), and 5) Adversarial Thinking (AT). (Burley, D. L. (JTF Co-Chair et al., 2017).

You may notice that the thought model dimension, *application areas*, is not depicted in *Figure 1,* and that is because it actually represents the link between the curricular content and the workforce framework (Burley, D. L. (JTF Co-Chair et al., 2017).

Introducing Frameworks
From the CSEC2017 thought model dimension, *knowledge areas,* we can map to what is referred to as Knowledge Units (KUs). KUs are part of another framework created by the National Centers of Academic Excellence in Cyber (CAE-CD), which happens to be a source and reference within CSEC2017.

The CAE-CD program is sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS), and as stated on the CAE Community website, "the goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in CD and producing a growing number of professionals with CD expertise in various disciplines." ("What is a CAE? | CAE Community," n.d., para. 2)

Another framework referenced in the CSEC2017 is one created by the National Initiative for Cybersecurity Education (NICE) which is led by the National Institute of Standards and Technology (NIST). NICE has created the Cybersecurity Workforce Framework (NICE Framework) which can be used as a reference and/or resource pertaining to the work and the knowledge, skills, and abilities (KSAs) needed for different cybersecurity positions within an organization (Newhouse, Keith, Scribner, & Witte, 2017).

According to Newhouse et. al (2017, p. 5), "The NICE Framework organizes cybersecurity and related work." This allows educators to easily identify the different KSAs that are needed to complete certain tasks.

KSAs and Those That Contain Linux
The NICE Framework defines KSAs by first defining work roles. Each KSA has been given an identification number (KSA ID), a description, and

©2017 ISCAP (Information Systems & Computing Academic Professionals)

ISSN: 2473-3857
v3 n4380

then mapped to work role(s) that need(s) the individual knowledge, skill, or ability. While there are many of these IDs, we singled out the KSAs and corresponding work roles that mentioned Linux. They are as follows:

K0224 – "Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems." (Newhouse et. al, 2017, p. 65) Work roles in need of K0224 include Technical Support Specialist, Vulnerability Assessment Analyst, Exploitation Analyst, Cyber Operator, and Cyber Defense Forensics Analyst.

K0397 – "Knowledge of security concepts in operating systems (e.g., Linux, Unix.)." (Newhouse et. al, 2017, p. 70). Work role includes Exploitation Analyst.

K0608 – "Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications)." (Newhouse et. al, 2017, p. 76). Work roles include Exploitation Analyst and Cyber Operator.

S0067 – "Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files)." (Newhouse et. al, 2017, p. 78). Work Roles include Law Enforcement/Counterintelligence Forensics Analyst and Cyber Defense Forensics Analysts

A0043 – "Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments." (Newhouse et. al, 2017, p. 89) Work role includes Cyber Defense Forensics Analyst.

Why The Focus on Linux

Besides the aforementioned KSAs that include Linux as a necessity to perform certain cyber security work roles, it is important to note that Linux takes up a hefty worldwide market share.

In fact, as stated in an article from 2015, the Linux operating system is utilized in more than ninety-seven percent of the world's supercomputers, eighty percent of smartphones, around seventy percent of all web servers, as well as other appliances and general desktop computers.(Cobbaut, 2015)

According to Finley (2016), every Android is run by Linux and many web applications and pages such as Facebook and Google are using it. Even Microsoft has let their guard down and is letting companies run Linux on its cloud computing service, Azure. Now "about one third of Azure instances are running Linux instead of Windows." (Finley, 2016, para. 8). Microsoft itself is using Linux behind the scenes for networking in Azure. It is so critical to web development that Microsoft partnered with Canonical, a Linux vendor, so developers could program Linux applications on their Windows computers (Finley, 2016).

There are several reasons why developers like Linux, but the main pull to it is the fact that it is open-source which means that anyone "can freely modify and redistribute its source code, tweaking it to better serve their own purposes." (Finley, 2016, p. 9). Companies can essentially customize their own version of Linux and the share (or sell) without permission (Finley, 2016).

The need to focus on Linux is credible just from the preceding references. It is all around us and is employed all over the world. When a tool is massively utilized in this way, there needs to be protections around the development process and ways to administer rules and policies to allow for safer application usage. This is why security education involving Linux is so important.

3. PURPOSE OF THE TOOLKIT

The purpose of the toolkit is to introduce virtual machine(s) and the Linux operating system to the absolute beginner. There is a need for more people who are interested in an ethical cyber security career due to a shortage of these professionals and the supply of security jobs continues to rise (Vogel, 2016).

To get students interested in difficult subjects, we need to break down the difficulty into easier-to-understand parts. This toolkit is a step-by-step manual that will guide the user to build his/her own virtual machines and will accompany a series of workshops. There will also be a more advanced manual and workshop series for those students who wish to continue from the beginner series as well as any new students who would like to join.

Beginners

The objective of the beginner manual is to introduce creating and using virtual machines as well as the command line of the Linux Operating System. There will be different distributions of Linux (Fedora, Ubuntu, and CentOS) that will be utilized to give some dimension to the training while allowing the users to familiarize themselves with more than one technology. This manual will

©2017 ISCAP (Information Systems & Computing Academic Professionals)

ISSN: 2473-3857
v3 n4380

suit the absolute beginner and will teach that person everything from where to download the Virtualbox hypervisor to editing files in the Linux terminal.

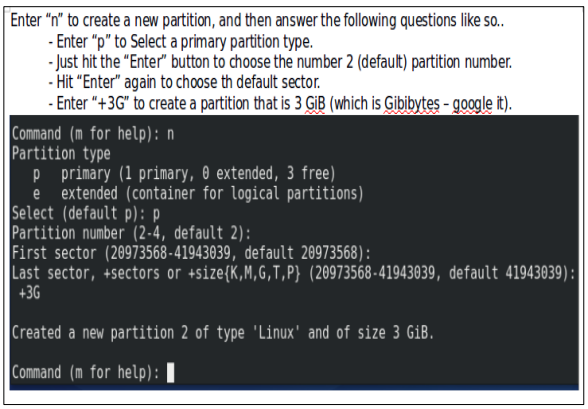

Figure 3 – The user is partitioning a virtual hard drive device called /dev/sda into four separate partitions.

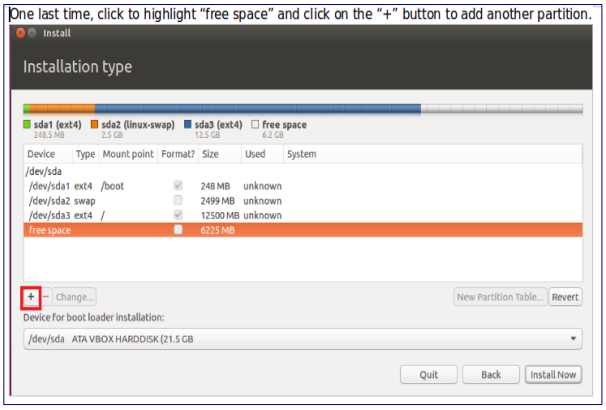

Figure 4 – Linux Toolkit - The user is using the command line interface to look at items within directories.

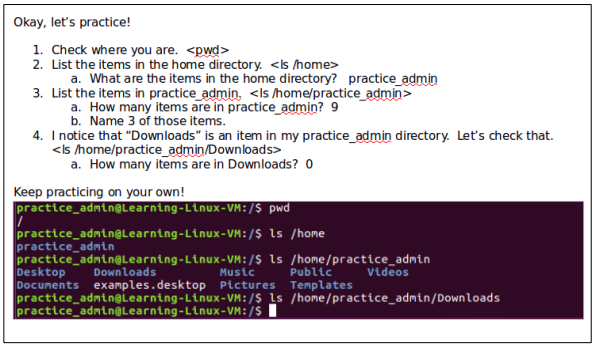

Figure 5 – Linux Toolkit - The user is creating a new primary 3 gibibyte partition.

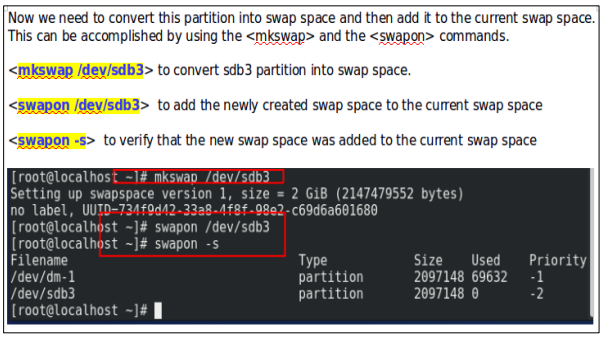

Figure 6 – Linux Toolkit - The user is converting a partition into swap space.

One will be able to install custom partitions using the GUI (Graphical User Interface – *Figure 3*) and check for items in certain directories (*Figure 4*). They will also be able to create custom partitions through the Linux command line (*Figure 5*) and swap filesystems (*Figure 6*).

By the end, they will be able to install a virtual machine, customize partitions via the GUI and the command line, make configuration changes to modify the grub menu, manage packages in Ubuntu and CentOS, perform queries using the different package managers, display system hardware, become familiar with the /dev, /sys and /proc directories, create and mount filesystems, manage filesystem quotas, edit default run-levels, monitor processes, list, copy and move files and directories, and manage text files.

The previous objectives will be listed out and explained in the manual. They will be practiced and implemented during the workshop portion of this Linux Toolkit. These knowledge, skills, and abilities will be the foundation for the next section of learning which will be the advanced manual and workshop series.

Advanced

The advanced manual will be a follow-up to the beginner manual. Any student that shows they have the knowledge or that went through the beginners manual and workshop is welcome to move forward to the advanced section. This section will start to align with certain techniques and commands system administrators may utilize in Linux like configuring X Windows, updating user and group accounts, system administration tasks, configuring locale and time zone settings, working with email, basic network configuration, security administration, securing data with encryption, host security, BASH (Bourne Again Shell) network configuration, BASH scripting, and

ISSN: 2473-3857
v3 n4380

working with a SQL (Structured Query Language) database.

These skills can be used to monitor activity to prevent possible attacks and will show the user how to stop and restore their system in the case they are attacked.

4. CONCLUSION

By creating a path to a cyber security career, the skill gap will begin to close as more students come out of academia prepared and ready for a cyber security career. Through implementation of the Linux Toolkit, we are contributing to the education of the future cyber security workforce and therefor also serving the need to close the knowledge, skills, and abilities gap as well as make the world incrementally safer while computing.

5. FUTURE STUDIES

During the spring semester, we will conduct a test and survey at the beginning and end of each workshop series. These tests and surveys will be given to the students to measure the effectiveness of the materials and curriculum for the workshops. This is so we can improve upon any discrepancies and/or any material that was unclear. We want to see how the toolkit impacts and improves the students overall Linux skills as well as their belief and feelings of their own skills.

6. REFERENCES

Burgess, M. (2017). That Yahoo data breach actually hit three billion accounts | WIRED UK. Retrieved October 19, 2017, from https://www.wired.co.uk/article/hacks-data-breaches-2017

Burley, D. L. (JTF Co-Chair, A., Bishop, M. (JTF Co-Chair, A., Buck, S. (ACM/CEP), Ekstrom, J. J. (IEEE C., Futcher, L. (ACM/IFIP), Gibson, C. D. (ACM/CEP), … Parrish, A. (IEEE C. (2017). *Cybersecurity Curricula 2017*. Retrieved from https://docs.wixstatic.com/ugd/895bd2_e3443415db4c432da8a66b59d076e151.pdf (page 18, 58, 66)

Cobbaut, P. (2015). Linux Fundamentals. Retrieved from http://linux- took-web-now-taking-world/ (page 1)

Finley, K. (2016). Linux Took Over the Web. Now, It's Taking Over the World | WIRED. training.be/linuxfun.pdf Retrieved August 15, 2017, from https://www.wired.com/2016/08/linux-

Krebs, B. (2014). The Target Breach, By the Numbers — Krebs on Security. Retrieved October 19, 2017, from https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Mapping ~ NSA/DHS Knowledge Unit to NICE Framework 2.0. (n.d.). Retrieved from https://niccs.us-cert.gov/sites/default/files/documents/pdf/mapping_nsa_dhs_knowledge_unit_to_nice_fw_2.0.pdf?trackDocs=mapping_nsa_dhs_knowledge_unit_to_nice_fw_2.0.pdf

McGee, M. K. (2017). A New In-Depth Analysis of Anthem Breach - BankInfoSecurity. Retrieved October 19, 2017, from https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *NIST Special Publication*, 800–181. https://doi.org/10.6028/NIST.SP.800-181 (page 5, 65, 70, 76, 78, 89)

Newman, L. H. (2017). The Biggest Cybersecurity Disasters of 2017 So Far | WIRED. Retrieved October 19, 2017, from https://www.wired.com/story/2017-biggest-hacks-so-far/

Spidalieri, F., & Kern, S. (2014). Professionalizing Cybersecurity: A path to universal standards and status. Retrieved from http://pellcenter.org/wp-content/uploads/2015/05/Professionalizing-Cybersecurity.pdf (page 8)

Vogel, R. (2016). CLOSING THE CYBERSECURITY SKILLS GAP. *Salus Journal*, *4*(2). Retrieved from http://www.salusjournal.com/wp-content/uploads/sites/29/2016/05/Vogel_Salus_Journal_Volume_4_Number_2_2016_pp_32-46.pdf (page 33

What is a CAE? | CAE Community. (n.d.). Retrieved August 14, 2017, from https://www.caecommunity.org/resources/what-cae (page 1)

©2017 ISCAP (Information Systems & Computing Academic Professionals)