2020

Technological Challenges and Innovations in Cybersecurity and Networking Technology Program

Syed R. Zaidi
CUNY Bronx Community College

Ajaz Sana
CUNY Bronx Community College

Aparicio Carranza
CUNY New York City College of Technology

Technological Challenges and Innovations in Cybersecurity and Networking Technology Program

Syed R. Zaidi†
Department of Engineering, Physics & Technology
Bronx Community College /CUNY
Bronx New York USA
syed.zaidi@bcc.cuny.edu

Ajaz Sana
Department of Engineering, Physics & Technology
Bronx Community College /CUNY
Bronx New York USA
Ajaz.Sana@bcc.cuny.edu

Aparicio Carranza
Computer Engineering Technology Department
New York City College of Technology/CUNY
Brooklyn New York USA
ACarranza@Citytech.cuny.edu

ABSTRACT

This era is posing a unique challenge to the Cybersecurity and related Engineering Technology areas, stimulated by the multifaceted technological boom expressed in accelerated globalization, digital transformation, the cloud, mobile access apps, and the Internet of Things (IoT)—where more and more devices are connected to the Internet every day. As the use of new Internet-based technologies increase; so does the risk of theft and misuse of sensitive information. This demands the awareness of cyber-criminality and the need for cyber hygiene in corporations, small businesses, and the government. As the need for experienced cybersecurity specialists has skyrocketed in recent years and employment for positions such as that of an information security analyst are projected to grow exponentially, there is a growing trend of cybersecurity training and certificate courses throughout the nation. Henceforth, this paper discusses the importance of designing a cybersecurity technology program, key challenges faced by it, and the use of advanced and innovative technologies to be employed. We will discuss various approaches to use technological innovation especially for advanced courses like Ethical Hacking and Network Penetration Testing and Computer Cybersecurity that include using cloud space to deploy virtual machines and labs; using VMware and the possibility of deploying Dell advanced VxR Hyperconverged System. This Software-defined architecture combines computing, storage, virtualization, management and has full-stack integration with VMware Technologies. This work is funded by the U.S Department of Education and CapitalOne Foundation grants and also includes consultation with National Cyberwatch and our key partner companies in this endeavor.

KEYWORDS

Cybersecurity, Hyperconverged, Virtualization, Networking.

1. Introduction

Cybersecurity, in general terms, refers to the development of techniques to protect the network, computers, smart devices, and information from damage or unauthorized access such as to satisfy the basic security goals of confidentiality, integrity, and availability. Cybersecurity and Network security continue to be a major concern of computer professionals today. There is limited availability of the cybersecurity workforce today. In this paper, we discuss the importance, need, and justification of the Cybersecurity program. Moreover, the technical and curriculum challenges to propose, design, and run such a cybersecurity and networking technology program at the Community College level, are also discussed.

2. Need and Justification

Network security continues to be a major concern of computer professionals today. Some of the key findings from Symantec's 2019 Internet Security Threat Report [1] are:

- One in ten URLs (Universal Resource Locator) is malicious.
- Web attacks are up 56%.
- 4,800 average websites are compromised each month with form jacking code.
- Enterprise ransomware is up 12% while mobile ransomware is up 33%.
- Supply Chain attack is up 78%.
- 48% of malicious email attachments are office files up from 5% in 2017.
- The number of attack groups using destructive malware is up 25% and the average number of organizations attacked by each group is 55.

According to Verizon's 2020 Data Breach Investigations Report, ransomware now accounts for 27% of all malware

incidents. Moreover, attacks on web apps were a part of 43% of breaches, more than double the results from last year [2]. A recent academic study suggests that using tremendous computing power and speed, no password is ultimately secure against a brute force attack [3]. A recent study by the University of Maryland suggests that there is a hacker attack every 39 seconds or, on average, 2,244 attacks each day [4].

As these types of attacks continue to accelerate, the need for trained security professionals also increases. Unlike some information technology functions, security is very difficult to offshore or outsource. It is important that individuals who want to be employed in the ever-growing field of information security be certified professionals. Recent employment trends indicate that employees with network security certificates/diplomas are in high demand. According to the 2019 (ISC)2 Global Information Security Workforce Study, the world's largest non-profit member association of certified cybersecurity security professionals, the first time estimated the current cybersecurity workforce as 2.8 million and the need for an additional trained workforce to close the gap is 4.07 million. The data demands of 145% more trained cybersecurity force. In the U.S., the current number of cybersecurity professionals is estimated to be 804,700 and the shortage is 498,490, necessitating an increase of cybersecurity trained workforce of 62%·[5].

The Department of Engineering, Physics, and Technology of Bronx Community College recognized the value of cybersecurity in the current era and proposed a new program leading to Associate in Applied Science in Cybersecurity and Networking. The Program was approved by NYSED in 2017. This degree has no parallel at our fellow CUNY institutions in the Bronx and no true parallel in CUNY.

3. Technological Challenges and Innovations in Curriculum Development

When the curriculum development was started at Bronx Community College then there were many technological challenges as there was no known program available at that time at the community college level. Moreover, since cybersecurity is a complex subject, it was challenging to design courses and prepare students for the cybersecurity industry that are freshmen from high school. A grant proposal was written at that time which was approved and our college was awarded a pilot grant from the Capital One Foundation to develop the program with the expectation of a full five years of funding support. Henceforth it was decided that the cybersecurity curriculum development team would be engaged in the DACUM (Developing a Curriculum) process. This is an information-gathering process that involves a panel of workers in the industry who are queried on their roles, tasks, responsibilities, skills, etc. The DACUM process helps ensure that the curriculum designed will provide the essential skills employers are seeking in new employees. Additionally, BCC will create a direct connection between industry and the classroom with the engagement of "industry faculty." Industry faculty will play an integral role in the design of the program, from updating curricula to serving on the advisory board. Further, industry faculty will receive pedagogical training and other forms of professional development, which is often uncommon for adjunct instructors.

Another innovation in this program is the bridge from non-credit certifications into a credit program ("stacking") e.g., Students already having valid A+ Certificate, can be granted credits against Computer Hardware and Software course in the program. Similarly, Network + can grant 3 credits against the Network Fundamentals course and so on, with up to 12 credits worth of relevant industrial certifications. We are confident that this will positively impact program outcomes, including retention and employment after graduation. This program can change how noncredit students are served going forward.

The program includes a sequence of technical core courses that provide hands-on knowledge and skills in systems, data, networking, and security concepts. Advanced course work includes training in PC hardware and operating systems, Windows servers, networking, routing, UNIX/LINUX operating systems, security, forensic analysis, encryption techniques, disaster recovery, and planning and virtualization. Students are prepared for industry certifications such as CCNA, A+, and Network+ in a hands-on lecture and laboratory environment. Cybersecurity is defined as the protection of computer systems from the theft or damage to the hardware, software, or the information on them, as well as from disruption or misdirection of the services they provide [6]. All data networks are comprised of four basic elements i.e.,

i. Hardware
ii. Software
iii. Protocols
iv. Connection Medium

On the other hand, elements of cybersecurity include:

i. Application security
ii. Information security
iii. Network security
iv. Disaster recovery/business continuity planning
v. Operational security
vi. End-user education

It is evident that the fundamentals of networking components serve as the foundation of cybersecurity, hence the proposed curriculum incorporates networking elements. Further, since BCC's Cybersecurity and Networking program is being informed by the Developing a Curriculum (DACUM) process, it ensures that our graduates have all the skills and training needed to succeed in their position after completing their degree. Moreover, to approve any program or curricular changes, it needs to be presented to the College Curriculum Committee which has a rule of at least three meetings, where a program is presented in detail and discussed before it can be approved by majority voting. The Curriculum Committee comprises of professors from all over the campus.

4. Technological Challenges and Innovations in the Lab Development

A very important part of the cybersecurity program, particularly, at the community college level is the hands-on training and practical expertise of the students. Cybersecurity programs are relatively new at the community college level. Henceforth, there are not many resources available, specifically at the time when we proposed the program. In order for the students to complete their lab or project work, it could be either a virtual or a hands-on approach. In a virtual approach all the lab exercises would be accomplished in a simulated environment whereas, in a hands-on approach, the students would be working directly on the physical equipment like routers, switches, etc. The virtual approach is faster and easier to deploy but it completely lacks the hands-on experience needed by the undergraduate students. On the other hand, due to the everyday challenges by the cybersecurity, software-defined networks (SDN), and virtualization, we cannot just rely on physical equipment. Hence we decided to use the hybrid-approach where we use the best of both worlds i.e., hands-on and simulation.

To efficiently design labs, we wrote another proposal and were awarded a grant of two years from the U.S. Department of Education to design and enhance our cybersecurity lab. A part of the grant is to be in-consultation with National Cyberwatch Center for guidance. National Cyberwatch Center is working for the development of Cybersecurity education programs under the grant funded by the National Science Foundation (NSF). After a thorough consultation with National Cyberwatch Center, InfoSec Learning LLC., Computacenter Inc., and Dell, we acquired simulation labs for our advanced cybersecurity major courses such as Ethical Hacking and Penetration Testing and purchased Dell VxRail Hyperconverged system in the process to deploy the latest Dell VxR Hyperconverged system. This Software-defined architecture combines computing, storage, virtualization, management and has full-stack integration with VMware Technologies. In other words, the Dell VxRail system is the easiest and fastest way to streamline and extend the VMware environment. Other advantages are resiliency, ease of deployment as it automates network setup. The Vxr system is built on PowerEdge servers. With a choice of 2nd Generation Intel® Xeon® Scalable or 2nd Generation AMD EPYC™ processors, VxRail is designed for today's mission-critical workloads in mind and also delivers multiple compute, memory, storage, network, and graphics options to cover a wide variety of applications and workloads. VxRail is a scalable distributed system consisting of common modular building blocks that allow users to start small with as little as 3 nodes which can be expanded up to 64 nodes in a cluster. This system requires at least three nodes to set up. Figure 1. Shows the configuration flexibility as per workload [7].

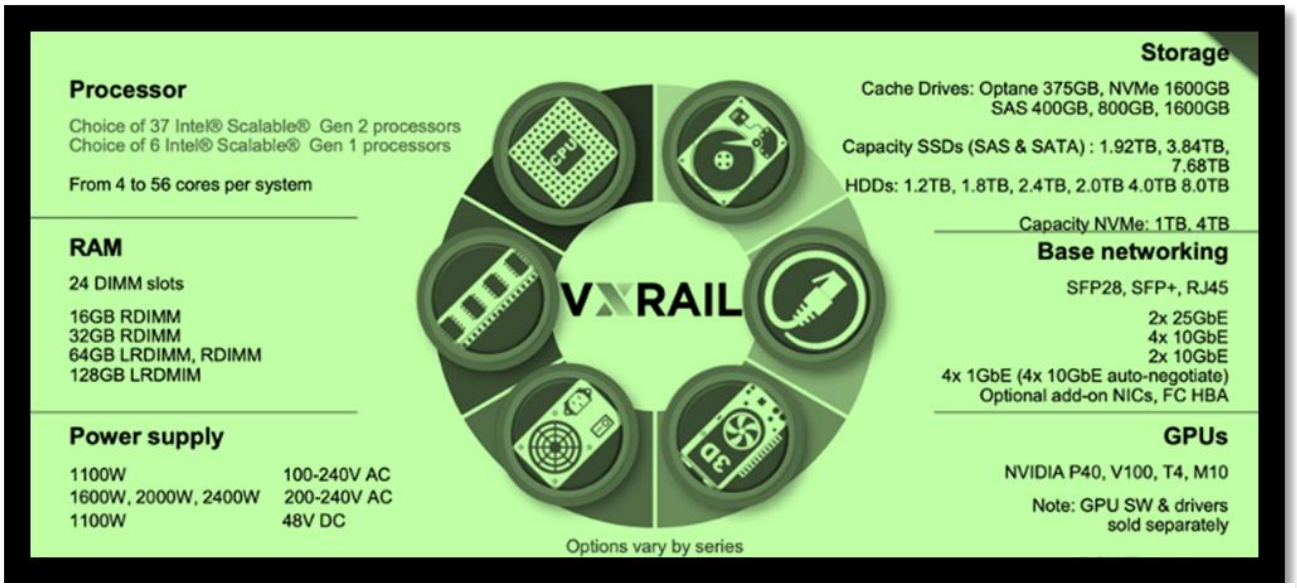

Figure 1: VxRail configuration flexibility as per workload.

VxR system obtained at Bronx Community College has 3 nodes, each node has 4 SSD drives, so there are 12 SSD drives offered by our system. The system needs 10 Gbps network connection through a switch with the availability of 6 ports operating at 10 Gbps. The system can be accessed within the network through VMware vCenter for simple deployment, extensibility, and scalability across the hybrid cloud, centralized control, and proactive optimization [8]. In this context, the cybersecurity lab will have the latest technology in place and will be streamlined with the industry.

5. Conclusion

This paper analyzes the significance of the Cybersecurity and Networking program at the associate degree level. It also discusses the curriculum design process and briefly described the designed courses topics. Important technological challenges and possible solutions are also evaluated. However, since almost all the activities of the college went virtual since the spring 2020 semester due to COVID-19, the equipment obtained couldn't be configured to reap all its benefits. Moreover, due to the varying challenges posed by cybersecurity worldwide, the program needs to be assessed regularly and should be flexible enough to incorporate any required changes.

ACKNOWLEDGMENTS

S. R. Zaidi would like to thank CapitalOne Foundation & U.S. Department of Education for their financial support and Dr. Alexander Ott (Associate Dean of Curriculum Matters & Academic Programs) and Dr, Jalil Moghaddasi (Chair) to help to design the Cybersecurity and Networking Technology Program and Julia Oliva (Director of grants and partnership) to help in the grant process at the Bronx Community College of the City University of New York (CUNY).

REFERENCES

[1] Symantec white paper, retrieved from, "https://docs.broadcom.com/doc/istr-24-2019-en", Published in 2019

[2] Verizon Data Breach Investigation Report, retrieved from, "https://enterprise.verizon.com/resources/reports/dbir/" Published 2020

[3] Katha Chanda, "Password Security: An Analysis of Password Strengths and Vulnerabilities", I.J. Computer Network and Information Security, 2016, 7, 23-30.

[4] A study report by the University of Maryland retrieved from, "https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds" Published 2020.

[5] 2019 (ISC)2 Global Cybersecurity Workforce Study 2019, retrieved from "https://www.isc2.org/Research/Workforce-Study"

[6] Gasser, Morrie (1988)," Building a Secure Computer System", Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. Retrieved from," http://cs2.ist.unomaha.edu/~stanw/gasserbook.pdf "

[7] Retrieved from, "https://infohub.delltechnologies.com/l/techbook-dell-emc-vxrail-system-2/intel-r-xeon-r-scalable-processor-powerful-processing-for-vxrail"

[8] Retrieved from, "https://www.vmware.com/products/vcenter-server.html"