The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #41272

Designing a Multi-VMs Platform for Infosec Students

Dr. Tarik Eltaeib, Farmingdale State College

Professor Tarik Eltaeib is a well-rounded, enthusiastic, highly accomplished, well-loved, natural leader and educator specializing in Computer Security, Operating systems and Security, and Computer Forensics. Professor Eltaib obtained his PhD in Computer Science and Engineering in May 2019 from the University of Bridgeport. His PhD thesis comprised ”Largescale Evolutionary Optimization using Multilayer Strategy Differential Evolution with AI and image processing application”. He obtained his Bachelor of Computer Science from the University of Garyounis (Benghazi) in 1999 and completed a Master of Computer Science and Information Technology Science in May 2010 from the same institution, completing a thesis on ”Health Informatics: Health Architecture based on SOA and Mobile Agents”. A great believer in continuing education and professional development for faculty members, he has earned new certifications and attended conferences, focusing on how to improve the learning experience for his students, as it can improve student outcomes by as much as 21%.He obtained the following relevant and important qualifications to strengthen his knowledge and skills in his chosen field:

Cisco Academy Accredited Instructor (CCNA, IT Essential I, IT Essential II) MCSA and MCSE certifications, making him officially Microsoft certified. Engaging Online Learners Grant Writing with Farmingdale Qualtrics CircleIn Application and Software

Professor Eltaeib has been invited as a Judge for Poster Presentations and is part of the IESC 2021 Organizing Committee: International Energy & Sustainability Conference 2021 (IESC 2021). This honor is a feather in his cap, acknowledging his skill and mastery of the subject and provides exposure to the broader academic community, not only for himself but also his department and school. He enhanced his career whilst studying by working in the private sector as a software developer in several companies and the Enterprise Application Administrator at a Mitsubishi Power Systems, where he built state-of-the-art Enterprise and Machine Learning Applications. Academic positions include Adjunct Professor at the University of Bridgeport, CT, and Assistant Professor – Computer Security where he is tenured at the School of Engineering Technology, Farmingdale State College - State University of New York. He has 6 years of higher education experience, and a total of 14 years. He has presented and published numerous conference papers, journal articles and contributed to a book chapter on Large-scale Evolutionary Optimization. He has excelled at going the extra mile, teaching not only his own classes but an additional Capstone projects, doing cybersecurity research, counseling students, assisting with open days for new students, contributing to curriculum enhancements, and proposing a new club to support women in the industry, SWCSI (Supporting Women in the Computer Security Industry). He excels at guiding students in subject choices based on interest, ability and skills. His continual quest for knowledge and broadening his skills has proven beneficial to his students and his professional evaluations reflect this in perfect teaching scores. Additional awards, societies and honor groups include:

2018 Expert Level Instructor Excellence Award – Cisco Networking Academy. 2017 Instructor 5 Years of Service Award – Cisco Networking Academy. 2017 Excellence in CCNA Curriculum Specialization Award – Cisco Networking Academy. 2017 Expert Level Instructor Award – Cisco Networking Academy. 2016 Expert Level Instructor Excellence Award – Cisco Networking Academy. 2015 Expert Level Instructor Excellence Award – Cisco Networking Academy. Member of the IEEE Computer Society since 2015.

Dr. M. Nazrul Islam, State University of New York

Dr. M. Nazrul Islam is a Professor at SUNY Farmingdale, where he is also serving as the Chairman of the Security Systems and Law Enforcement Technology Department. He has been in the academia since 1991 and worked at several renowned institutions, inc

Dr. Qinghai Gao

Cybersecurity Online Virtual Machine Lab -COVML
Designing a Multi-VMs platform for Infosec Students

Tarik Eltaeib
Eltaeit@farmingdale.edu

Nazrul Islam
islamn@farmingdale.edu

Qinghai J. Gao
gaoqj@farmingdale.edu

Keyword: computer security-cybersecurity education – information security skills

Absrtact

Effective cybersecurity education requires a pragmatic approach to guarantee that students not only comprehend theoretical principles but also can implement them. Conventional lecture-based education is inadequate in conveying the dynamic nature of network-based attack and response techniques. This research aims to fill this need by examining the incorporation of testbed networks and live exercises into a network security curriculum.

1. Introduction

Learning information security can be challenging for new students, regardless of their background. Various factors contribute to the complexity of the field. Information security is filled with technical terminology and acronyms, which can be rough for new students to understand. Also, understanding computer networking, software execution, and operating systems is crucial for comprehending information security concepts[1]. Information security is always evolving as new threats and technologies emerge. Continuous learning and adaptability are needed to keep up. Mastering information security is a daunting task for all students, irrespective of their background[2]. Concepts such as networking and software execution pose significant challenges that require a great deal of effort to overcome.

A virtual machine (VM) is a piece of technology that lets you build a model computer within your actual computer[3]. It enables the simultaneous use of numerous operating systems on a single computer. If your main computer runs Windows, for instance, you may use a virtual machine (VM) to run Linux or another operating system on the same hardware[4]. Without the need for separate physical machines, this virtualization technology offers flexibility and agility for a variety of jobs, including software testing.

Online virtual machines offer a secure and efficient way to work with different operating systems, irrespective of the locally installed operating system[5]. This enables students to perform complex tasks and run software that may not be compatible with their primary operating system without the risk of exposing the underlying system to cyber threats[6]. Moreover, virtual machines provide a safe environment for conducting experiments and testing applications without affecting the integrity of university lab computers.

Also, the development of e-learning has transformed the education sector by providing a flexible and individualized approach, which frequently stands in stark contrast to the inflexibility of old educational approaches[7]. This kind of learning has thrived especially in diverse areas, such as IT security education. Nevertheless, e-learning in IT security education encounters a notable obstacle: the issue of delivering practical experience owing to the absence of physical closeness.

In the field of IT security education, online laboratory settings and practical exercises are not only advantageous, but also vital[8]. These tools enable students to use theoretical knowledge in practical situations, fostering the acquisition of essential skills necessary for their professional advancement and expertise in the respective subject[9]. Regrettably, the traditional arrangement of computer labs in IT security education is burdened with constraints, notably regarding lack of mobility and the exorbitant expenses linked to their establishment and upkeep[10].

Consequently, it is essential to convert security labs and practical exercises into e-learning forms. This change is not without its problems. Simulating authentic IT security settings and situations in a virtual realm necessitates the use of new techniques. To effectively address IT security concerns, it is crucial to create e-learning platforms that include both interactivity and user-friendliness, while also being strong enough to accurately replicate the intricate and ever-changing nature of these difficulties[10, 11].

Learning information security can be challenging, regardless of one's background. Various factors contribute to the complexity of the field. Information security is often filled with technical terminology and acronyms that can be difficult for new students to understand[12]. Additionally, understanding computer networking, software execution, and operating systems is crucial for comprehending information security concepts. Information security is constantly evolving, and new threats and technologies continuously emerge. Therefore, continuous learning and adaptability are essential to keep up with the changes[13]. Mastering information security can be daunting for all students, and concepts such as networking and software execution pose significant challenges that require much effort.

A virtual machine (VM) is a technology that allows building a model computer within the actual computer. It enables the simultaneous use of multiple operating systems on a single computer. For instance, if your main computer runs Windows, you may use a virtual machine (VM) to run Linux or another operating system on the same hardware[14]. This virtualization technology provides flexibility and agility for various tasks, including software testing, without requiring separate physical machines.

Online virtual machines offer a secure and efficient way to work with different operating systems, regardless of the locally installed operating system. the development of a Cybersecurity Online Virtual Machine Lab (COVML) that offers desktop virtualization, allowing a desktop operating system to be executed and controlled on a server in a data center. This enables students to perform complex tasks and run software that may not be compatible with their primary operating system without the risk of exposing the underlying system to cyber threats[15]. Moreover, virtual machines provide a safe environment for conducting experiments and testing applications without affecting the integrity of university lab computers[16].

We propose the development of a Cybersecurity Online Virtual Machine Lab (COVML) that offers desktop virtualization, allowing a desktop operating system to be executed and controlled on a server in a data center.

A COVML, or Computer-based Virtual Modeling and Learning, is a digital environment often used for the purposes of teaching, practicing, or doing research in the field of cybersecurity. These laboratories provide a controlled and separated environment where users may acquire knowledge and conduct experiments related to different cybersecurity ideas and techniques, without exposing real systems or networks to any potential damage.

Users may access the desktop on COVML from a variety of devices, such as thin clients, PCs, or other devices, across a network. This enables the consolidation of desktop administration, enhanced security, and perhaps decreased expenses related to hardware.

Designing a platform with multiple virtual machines for information security students to gain practical experience and necessary skills. In information security education, this platform is a valuable tool for students to enrich their learning experience[17]. Providing a practical learning environment enables students to apply theoretical knowledge to real-world scenarios, effectively preparing them for a career in cybersecurity. This platform facilitates a comprehensive approach to learning, encompassing theoretical concepts and practical skills, ultimately ensuring a well-rounded education in information security[18].

A COVML, or Computer-based Virtual Modeling and Learning, is a digital environment often used for the purposes of teaching, practicing, or doing research in the field of cybersecurity. These laboratories provide a controlled and separated environment where users may acquire knowledge and conduct experiments related to different cybersecurity ideas and techniques, without exposing real systems or networks to any potential damage[19, 20]. The following the advantage of A COVML, or Computer-based Virtual Modeling and Learning:

Users may access the desktop on COVML from a variety of devices, such as thin clients, PCs, or other devices, across a network. This enables the consolidation of desktop administration, enhanced security, and perhaps decreased expenses related to hardware.

Hands-On Learning: Interact with natural operating systems, applications, and network configurations in a controlled environment to gain practical experience[21].

Experimentation: Students can explore security scenarios and vulnerabilities by testing various security programs, tools, and configurations[22].

Skill Development: Develop essential cybersecurity skills such as network security, system hardening, malware analysis, penetration testing, and incident response[23].

Real-World Simulation: Simulate real-world cybersecurity threats, allowing students to apply their knowledge in practical scenarios[24].

Safe Environment: Learn and experiment in a safe, isolated environment without risking natural systems or networks[4].

Also, Diverse Environments deals with various operating systems and network setups by working with different IT landscapes. Collaboration which teamwork and problem-solving skills by participating in group projects, penetration testing exercises, or capture-the-flag (CTF) competitions with your peers. A COVML provides a continuous learning platform allows individuals to keep learning and refining their skills at any time[25]. This is particularly useful in fields where new technologies and threats are constantly emerging. Scalability is another important feature of a COVML which is crucial to accommodate the increasing number of students and evolving educational needs[7].

It is essential to teach students about ethical cybersecurity practices. This will provide them with the necessary skills to responsibly test and secure computer systems. By emphasizing the importance of ethical behavior in cybersecurity, we can help to create a culture of trust, integrity, and responsibility in the field. This will benefit individual students and contribute to a more secure and stable digital landscape for all users[7, 26].

2. COVML Safe Environment for Learning and Testing:

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, damage, or theft. VM laboratories provide a distinct and essential setting for education and experimentation, particularly in the field of information security. These laboratories provide a secure environment where users may explore many facets of cybersecurity without the inherent dangers connected with real-world systems. The significance of this facet of cybersecurity training is crucial for several reasons[27].

2.1 Exploration of Malicious Software

Malware Analysis in Cybersecurity VM Lab: A significant advantage of using a cybersecurity virtual machine laboratory is the capacity to securely manage and examine malicious software. Within a regulated virtual setting, individuals can analyze and deconstruct viruses, worms, ransomware, and other forms of malicious software to comprehend their mechanisms, without the danger of these harmful entities propagating to actual networks or systems[28].

2.2 Practicing Hacking Techniques

Dealing in Hacking Techniques: Ethical hacking is an essential proficiency in the field of cybersecurity, used for defensive and proactive objectives. Virtual machine laboratories provide a controlled environment for both novice and seasoned cybersecurity experts to hone their skills in hacking methodologies, including penetration testing and vulnerability exploitation. Gaining practical experience is essential for comprehending the methods used by attackers and improving defense mechanisms against such assaults[29].

2.3. Realistic Scenarios Without Real-World Consequences:

Simulated Scenarios with Authenticity and No Actual Ramifications: These laboratories may be customized to replicate many genuine networks and systems, offering a genuine setting for cybersecurity drills. The primary benefit is in the fact that any unauthorized access, loss of data, or malfunction that happens inside the virtual laboratory does not result in actual repercussions, therefore enabling more assertive experimentation and knowledge acquisition[30].

2.4 Learning from Mistakes

Gaining expertise through failures plays an important role in the field of cybersecurity. VM laboratories provide a lenient setting where errors are not only tolerated but also considered an important component of the learning process. Users may acquire knowledge from these blunders without experiencing the stress or apprehension of inflicting actual harm[30, 31].

3. COVML Tools and Resources

Virtual Machine (VM) laboratories serve as secure environments that function as resource hubs, offering a diverse range of tools and resources necessary for conducting security testing and analysis. These technologies are essential for the learning and practice process in cybersecurity, providing users with the ability to do comprehensive and efficient security assessments. Below is a summary of the many sorts of instruments and materials often available in these laboratories[32].

3.1 Vulnerability Scanners:

Vulnerability scanners, such as Nessus or OpenVAS, are automated tools used to scan systems and networks to identify and assess known vulnerabilities. They assist in discovering vulnerabilities in security measures, such as obsolete software, absent updates, or incorrect setups[33].

3.2 Forensics Tools:

Cybersecurity includes the examination and evaluation of cybercrimes. Autopsy and EnCase are used in the field of digital forensics to retrieve and examine data from digital media. This process is essential for comprehending the cause of a security breach and collecting evidence[34].

3.3Intrusion Detection Systems (IDS):

Intrusion Detection Systems (IDS): Tools such as Snort are used to oversee network traffic, detecting any anomalous behavior or breaches in security. They are crucial for acquiring the skills necessary to identify and promptly react to malevolent actions in real-time[32].

3.4 Web Application Security Tools

Given the widespread use of web-based services, it is essential to use tools such as OWASP ZAP and Burp Suite to assess the security of online applications. They assist in detecting prevalent vulnerabilities such as SQL injection, cross-site scripting, and other security deficiencies in online applications[35].

3.5 Security Information and Event Management (SIEM) Systems, such as Splunk or ELK Stack, are used to do immediate analysis of security alarms produced by applications and network devices. They are essential for comprehending the broader scope of network security[32].

3.6 Scripting and Programming Tools: Capability in scripting and programming tools is crucial for cybersecurity. Laboratories often include development tools for the purpose of authoring, evaluating, and executing scripts or programs that automate security duties or analyze data[36].

3.7 Sandbox Environments: To safely analyze malware, sandboxing tools are used to isolate malicious software in a secure environment to observe its behavior without risking the lab's integrity[22].

4-The architecture of a Cybersecurity Online Virtual Machine Lab (COVML) Architecture

The COVML architecture plays a vital role in virtualization technology, allowing multiple operating systems to run simultaneously on a single physical hardware host. This is made possible by creating a virtual machine that emulates the hardware of a physical machine, including its processor, memory, storage, and network interfaces. The virtual machine is isolated from the host machine, which means that the operating systems running on it are also isolated from one another[36]. This isolation provides security and prevents interference between the multiple operating systems sharing the same hardware.

The COVML architecture achieves this by using a hypervisor, a software layer between the host machine's physical hardware and the virtual machines. The hypervisor manages allocating resources to each virtual machine and coordinates communication between them[18]. The COVML architecture is a crucial component of virtualization that enables efficient use of hardware resources by allowing multiple operating systems to coexist on a single physical machine.

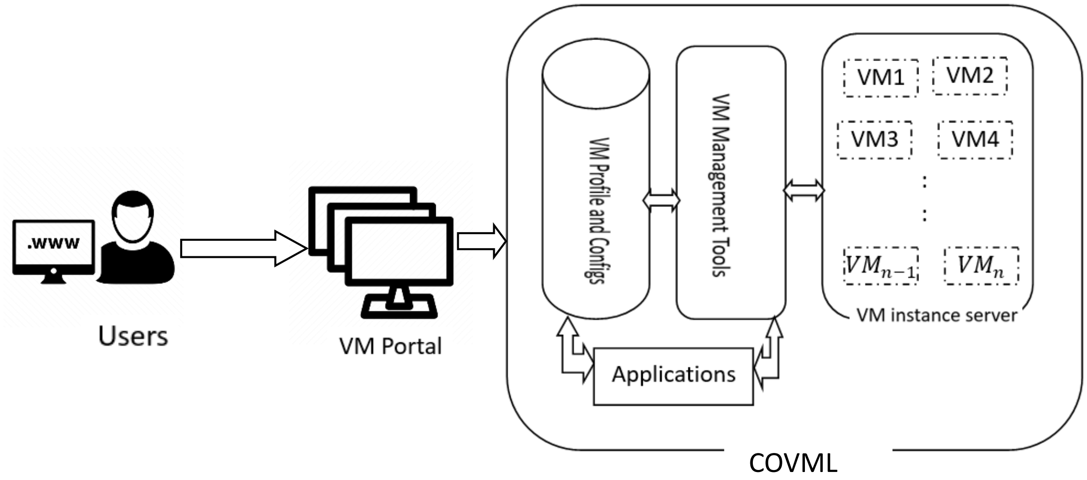

Figure 1.1 a Cybersecurity Online Virtual Machine Lab (COVML) Architecture

4.1VM Profile and configs:

A VM profile is a collection of specifications and configurations that describe the hardware and software attributes of a virtual machine. It includes details such as the amount of memory, the number of CPUs, the size and type of storage, the operating system, and any installed software[7]. A VM profile is essential for creating and managing virtual machines as it provides a blueprint for the desired configuration. By defining a VM profile, users can ensure that their virtual machines have the necessary resources to run their applications and perform their intended tasks efficiently.

4.2Virtual Machine (VM) management

Virtual Machine (VM) management tools are software programs specifically developed to oversee and maintain virtual machines inside a virtualized environment. These technologies provide capabilities for generating, altering, monitoring, and overseeing virtual machines (VMs) on various hosts and clusters[35]. Below is a summary of many widely used virtual machine (VM) management tools and their respective functionalities.

5. Conclusion:

Cybersecurity Virtual machine laboratories are an essential instrument in the realm of information security education and practical application[31]. They provide a protected and regulated setting in which the perilous and sometimes hazardous components of cybersecurity jobs may be examined and executed securely and efficiently. Practical experience is essential for acquiring the skills and knowledge necessary to safeguard against and address cyber dangers in real-life situations.

The integration of these tools and resources inside a Cybersecurity VM lab offers a full array for training, experimentation, and skill development in many areas of cybersecurity. They enable learners and practitioners to stay ahead in the rapidly evolving field of cybersecurity by offering hands-on experience with the tools and techniques used in real-world scenarios.

Reference

1. Aziz, E.-S., S.K. Esche, and C. Chassapis, *Design and implementation of a virtual laboratory for machine dynamics.* International Journal of Online Engineering, 2010. **6**(2).
2. Le, T., *A survey of live virtual machine migration techniques.* Computer Science Review, 2020. **38**: p. 100304.
3. Hu, J., D. Cordel, and C. Meinel, *A virtual machine architecture for creating it-security laboratories*. 2006: Universitätsverlag Potsdam.
4. Goldberg, R.P., *Survey of virtual machine research.* Computer, 1974. **7**(6): p. 34-45.
5. Ragsdale, D., S. Lathrop, and R. Dodge, *Enhancing information warfare education through the use of virtual and isolated networks.* Journal of Information Warfare, 2003. **2**(3): p. 47-59.
6. Sedjelmaci, H., et al., *Cyber security based on artificial intelligence for cyber-physical systems.* IEEE Network, 2020. **34**(3): p. 6-7.
7. Robles-Gómez, A., et al., *Emulating and evaluating virtual remote laboratories for cybersecurity.* Sensors, 2020. **20**(11): p. 3011.
8. Vigna, G., *Teaching hands-on network security: Testbeds and live exercises.* Journal of information warfare, 2003. **2**(3): p. 8-24.
9. Li, C., et al. *BAC: Bandwidth-aware compression for efficient live migration of virtual machines*. in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. 2017. IEEE.
10. Helali, L. and M.N. Omri, *A survey of data center consolidation in cloud computing systems.* Computer Science Review, 2021. **39**: p. 100366.
11. Li, B., B. Li, and F. Liu, *Cloud and data center performance [Guest Editorial].* IEEE Network, 2013. **27**(4): p. 6-7.
12. Topham, L., et al., *Cyber security teaching and learning laboratories: A survey.* Information & Security, 2016. **35**(1): p. 51.
13. Reece, R. and B.C. Stahl, *The professionalisation of information security: Perspectives of UK practitioners.* Computers & Security, 2015. **48**: p. 182-195.
14. Masrek, M.N., et al. *The role of top management in information security practices*. in *The 6th International Conference on Education, Social Sciences and Humanities, Istanbul, Turkey*. 2019.
15. Rahman, N.A.A., et al., *The importance of cybersecurity education in school.* International Journal of Information and Education Technology, 2020. **10**(5): p. 378-382.
16. Bada, M. and J.R. Nurse, *Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs).* Information & Computer Security, 2019. **27**(3): p. 393-410.
17. Ponomareva, O., et al. *Global Training of Professionals in the Area of Information Security*. in *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*. 2020. IEEE.

18. Dutta, N., et al., *Design of a virtual cybersecurity lab.* Cyber Security: Issues and Current Trends, 2022: p. 143-157.

19. Tong, Y.J., W.Q. Yan, and J. Yu, *Analysis of a secure virtual desktop infrastructure system.* International Journal of Digital Crime and Forensics (IJDCF), 2015. **7**(1): p. 69-84.

20. Rehman, A., et al., *Virtual machine security challenges: case studies.* International Journal of Machine Learning and Cybernetics, 2014. **5**: p. 729-742.

21. AlMutair, L. and S. Zaghloul. *A new virtualization-based security architecture in a cloud computing environment*. in *3rd international conference on digital information processing and communication, Dubai, UAE*. 2013.

22. Kazim, M., et al. *Security aspects of virtualization in cloud computing*. in *Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013. Proceedings*. 2013. Springer.

23. Park, J.H. *A virtualization security framework for public cloud computing*. in *Computer Science and its Applications: CSA 2012*. 2012. Springer.

24. Jyoti, S., S. Manish, and G. Rupali. *Virtualization as an engine to drive cloud computing security*. in *International Conference on High Performance Architecture and Grid Computing*. 2011. Springer.

25. Hasneen, J., V. Narayanan, and K.M. Sadique. *A Systematic Literature Review on Security Aspects of Virtualization*. in *International Conference on Hybrid Intelligent Systems*. 2022. Springer.

26. Caminero, A.C., et al., *Virtual remote laboratories management system (tutores): using cloud computing to acquire university practical skills.* IEEE transactions on Learning Technologies, 2015. **9**(2): p. 133-145.

27. García, I.A., C.L. Pacheco, and J. Garcia, *Enhancing education in electronic sciences using virtual laboratories developed with effective practices.* Computer Applications in Engineering Education, 2014. **22**(2): p. 283-296.

28. Caminero, A., et al. *Obtaining university practical competences in engineering by means of virtualization and cloud computing technologies*. in *Proceedings of 2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*. 2013. IEEE.

29. Wang, Y., M. McCoey, and Q. Hu. *Developing an undergraduate course curriculum for ethical hacking*. in *Proceedings of the 21st Annual Conference on Information Technology Education*. 2020.

30. Al Kaabi, S., et al. *Virtualization based ethical educational platform for hands-on lab activities on DoS attacks*. in *2016 IEEE Global Engineering Education Conference (EDUCON)*. 2016. IEEE.

31. Willems, C., et al. *A distributed virtual laboratory architecture for cybersecurity training*. in *2011 International Conference for Internet Technology and Secured Transactions*. 2011. IEEE.

32. Willems, C. and C. Meinel. *Online assessment for hands-on cyber security training in a virtual lab*. in *Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON)*. 2012. IEEE.

33. Soceanu, A., M. Vasylenko, and A. Gradinaru. *Improving cybersecurity skills using network security virtual labs*. in *Proceedings of the International MultiConference of Engineers and Computer Scientists*. 2017.

34. Ksiezopolski, B., et al. *Hands-on Cybersecurity Labs in online learning*. in *EdMedia+ Innovate Learning*. 2021. Association for the Advancement of Computing in Education (AACE).

35. de Leon, D.C., et al., *Tutorials and laboratory for hands-on OS cybersecurity instruction.* Journal of Computing Sciences in Colleges, 2018. **34**(1): p. 242-254.

36. Olmsted, A. *Scalable Undergraduate Cybersecurity Curriculum Through Auto-graded E-Learning Labs*. in *Advances in Software Engineering, Education, and e-Learning: Proceedings from FECS'20, FCS'20, SERP'20, and EEE'20*. 2021. Springer.