

Article

Advanced Network and System Security Teaching

Mihajlo Ogrizović ^{*,†} , Pavle Vuletić [†]  and Žarko Stanisavljević 

School of Electrical Engineering, University of Belgrade, 11000 Belgrade, Serbia; pavle.vuletic@etf.bg.ac.rs (P.V.); zarko.stanisavljevic@etf.bg.ac.rs (Ž.S.)

* Correspondence: ogrizovic@etf.bg.ac.rs

[†] These authors contributed equally to this work.

Abstract: In an attempt to address the growing shortage of cybersecurity specialists in the country, the School of Electrical Engineering, University of Belgrade, started the course entitled Advanced Network and System Security (ANS) in the 2019/2020 school year. The ANS course covers the topics of computer system and network security, intrusion detection and prevention, and ethical hacking methodologies. This paper presents the course organization and associated laboratory environment and exercises and aims to prove that providing such a multidisciplinary laboratory leads to successful learning outcomes and directly improves gained knowledge in cybersecurity. The ANS course differs from all other related courses by covering various cybersecurity topics ranging from hardware through to network to web security. The analysis showed that 13 out of 19 Cyber Security Body of Knowledge classification Knowledge Areas are covered in the ANS course, unlike other related courses which cover up to 8 Knowledge Areas. Ultimately, the students' practical skills improvement evaluation was performed through quantitative and qualitative analysis in order to prove that improving practical skills in the ANS laboratory resulted in the overall improvement of the gained knowledge.

Keywords: architecture for educational technology systems; cybersecurity education; evaluation methodologies; network security; system security



Academic Editor: Christos J. Bouras

Received: 15 November 2024

Revised: 8 December 2024

Accepted: 15 December 2024

Published: 24 December 2024

Citation: Ogrizović, M.; Vuletić, P.; Stanisavljević, Ž. Advanced Network and System Security Teaching. *Electronics* **2025**, *14*, 3. <https://doi.org/10.3390/electronics14010003>

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Destructive cyber-attacks have evolved and expanded dramatically. The dynamic nature of the technological landscape and the creativity and unpredictability of attackers make cyber-attacks a continuously increasing global threat. Predictions say that global damage costs only from one type of attack—ransomware—will likely exceed USD 265 billion by 2031 [1]. This causes an increased demand for cybersecurity specialists. However, according to recent cybersecurity workforce reports [2], there is a significant and growing shortage of cybersecurity specialists worldwide. In an attempt to bridge this gap as soon and as efficiently as possible, the School of Electrical Engineering, University of Belgrade (SEE-UB), created the Advanced Network and System Security (ANS) course through the Erasmus Capacity Building in Higher Education Program [3] which funded the project Information Security Services Education in Serbia (ISSES) [4]. The project aimed to create several master's degree courses in information security, which would be either incorporated into existing master's degree programs or offered as completely new master's degree programs at major Serbian universities. The SEE-UB, among others, was responsible for creating an introductory master's degree course in cybersecurity.

Various attack vectors that exist in the present day, which include exploiting vulnerabilities in hardware, firmware, operating systems, network protocols, and mechanisms and applica-

tions, require significant prior knowledge in various computer science topics. This, but also a multitude of attack approaches and examples that should be demonstrated to students, makes preparing and organizing such a course and evaluating the intended level of understanding and learning outcomes very challenging. Finally, the ANS course's goal was to provide students with practical skills similar to the ones obtained in the Certified Ethical Hacker (CEH) program [5] covering a wide range of cybersecurity topics. Preparing a laboratory environment and a set of laboratory exercises for such a course differs from the practice seen so far at universities which typically have laboratories dedicated to a specific and narrow-scoped topic (e.g., network laboratory, web application laboratory, etc.). As we show in Section 2 of this paper, the practical part of the ANS course, its multidisciplinary information security laboratory, and the modularity of the laboratory environment that is elastic and highly extensible are unique and the most comprehensive so far compared to the other university courses.

The ANS course was held at the SEE-UB for the first time in the 2019/2020 school year. The number of students who elected the course was between 32 and 112 per school year in the first four school years, reaching its peak in 2021/2022. During the past four years, the practical part of the course has increased the number of laboratory exercises from 7 to 20, providing more emphasis on the practical work. In this period, over 93% of students (who participated in anonymous surveys about their experience) were satisfied with the course. This paper aims to share the experience in organizing the ANS laboratory and prove that providing such a multidisciplinary laboratory leads to successful learning outcomes and directly improves gained knowledge in cybersecurity.

The main contributions of this paper are a description of the ANS course with a focus on the practical part of the course and a thorough analysis of learning outcomes with the use of such a multidisciplinary cyber security laboratory environment. Another contribution is a thorough review of related work and comparison with the ANS course based on the coverage of the topics and the development characteristics of the laboratory environment.

The rest of the paper is organized as follows. Section 2 provides an overview of related work and compares the ANS course to other related courses based on the laboratory environment's topic coverage and development characteristics. Section 3 describes the novel ANS course and the laboratory environment and exercises. Section 4 gives students' practical skills' improvement evaluation through quantitative and qualitative analysis. Section 5 concludes the paper.

2. Related Work

This section presents a thorough survey of the existing work in cybersecurity education, with a focus on cybersecurity education laboratory environments, which will be presented in the following subsections through different comparisons.

2.1. Search Process

A systematic search across multiple academic databases was conducted to compile a comprehensive list of related work, including Google Scholar, SpringerLink, IEEE Xplore, ACM Digital Library, and Elsevier. The initial search was only conducted on papers published in well-known and well-regarded journals on computer education, specifically Computers and Education, IEEE Transactions on Education, ACM Transactions on Computing Education, and Computer Applications in Engineering Education. The search was initiated this way to ensure more papers that fit the search criteria presented below and, therefore, find related work more efficiently.

The search was conducted by searching the paper archives with the keywords cybersecurity and security and broadened by selecting and reviewing the papers that referenced

the initially found papers. Along with this, the search was widened by finding papers that fit the search criteria that included the following words:

“Security” OR “Cyber Security” OR “Cybersecurity”) AND (“Environment” OR “Laboratory” OR “Education”)

This resulted in a total of 92 papers being further examined. Each paper found was analyzed through three elimination steps:

1. An analysis and comparison of the paper’s title with selection criteria;
2. An analysis and comparison of the paper’s abstract with selection criteria;
3. An analysis and comparison of the paper itself with selection criteria.

After this phase, 31 papers were excluded from the analysis because the presented laboratory environment was aimed at a different user group. For example, papers like [6,7] present novel ways of educating children and sub-university level teenagers. Another reason for exclusion was that the focus of a paper was on areas that are not grounded in computer science (e.g., [8] or [9]). The full set of analysis criteria can be seen in Table 1. Out of the remaining 61 publications, 16 were not presented in the comparisons because they were review papers or papers that did not present new learning methodologies in cybersecurity. However, they were used to expand the search for other valuable publications for this research and to construct criteria for comparing the presented laboratory environments in the selected papers [10–25].

As mentioned, the laboratory environment that is presented in this paper is part of a course for students with a bachelor’s knowledge in computer science (this is a course on a master’s degree program at the SEE-UB), as well as basics in Data Protection. That is why only educational papers focusing on laboratory environments used to teach students with prior knowledge of computer science as well as programs used by companies to teach workers about security hazards were taken into account.

Table 1. Inclusion criteria for this paper.

Type of Criteria	Inclusion Criteria	Excluded
Content	The laboratory environment presented in the publication targets adults with solid computer science or software engineering knowledge.	[6–9,26–31]
Content	The publication presents a novel laboratory environment or tool used for cybersecurity or network educational purposes.	[32–52]
Language	The literature is in English	/
Access	The full paper can be accessed	/
Bibliographic information	The source was published after 2005.	/

The comparison was based on two criteria: covering topics in the ANS cybersecurity course and cybersecurity courses that were elaborated in the related papers and the architecture and deployment technology of the ANS cybersecurity educational laboratory environment and cybersecurity environments presented in other papers.

1. Covering topics in the ANS cybersecurity course and cybersecurity courses that were elaborated in the related papers;
2. The architecture and deployment technology of the ANS cybersecurity educational laboratory environment and cybersecurity environments presented in other papers.

A more detailed explanation of how the key characteristics of each criterion were chosen, as well as the comparison itself, are shown in the following subsections. The key characteristics of the papers and laboratory environments described in them were extracted by gathering information directly from the papers (and the corresponding appendices

and accompanying information if there were any). As will be observed in the following chapters, some characteristics of the environments remain undefined, which is due to the inability to derive these features solely from the content of the papers or the accompanying information or appendices.

2.2. Comparison Based on Covered Topics

Several previous papers classify and compare security learning laboratories and cybersecurity courses. Papers like [13,15,21] rely on the CSEC 2017 Guidelines [53] and others rely on the NIST NICE Framework [16,20]. Some papers like [14,22] even propose new capability assessment methodologies.

The classification used in this paper was created by the Cyber Security Body of Knowledge (CyBOK) and is based on its Knowledge Areas. It is explained in detail in [19] and was developed by world experts and therefore aligns with current cybersecurity trends and needs. The reason for using the CyBOK classification instead of the already-mentioned ones is that this classification is based on different types of cyber attacks, which is more the focus of the ANS course, while the frameworks mentioned in the previous paragraph focus more on different types of cyber defense strategies. There are 19 proposed Knowledge Areas, which are presented in Table 2.

Table 2. Overview of Knowledge Areas.

Risk Management and Governance (KA1)	Operating Systems and Virtualization Security (KA10)
Law and Regulation (KA2)	Distributed Systems Security (KA11)
Human Factors (KA3)	Authentication, Authorization, and Accountability (KA12)
Privacy and Online Rights (KA4)	Software Security (KA13)
Malware and Attack Technologies (KA5)	Web and Mobile Security (KA14)
Adversarial Behaviors (KA6)	Secure Software Lifecycle (KA15)
Security Operations and Incident Management (KA7)	Network Security (KA16)
Forensics (KA8)	Hardware Security (KA17)
Cryptography (KA9)	Cyber-Physical Systems Security (KA18)
Physical Layer and Telecommunications Security (KA19)	

The mentioned Knowledge Areas were used as classifications in Table 3, with one modification to improve classification granularity. Namely, several laboratory environments are focused on Web Security, showing and simulating attacks on Web Applications and servers. Therefore, those laboratory environments would be classified by the CyBOK classification as having covered Web and Mobile Security (KA14). However, none of these laboratory environments cover Mobile Security. Therefore, to display a classification with more granularity, KA14 was divided into two columns: Web Security (KA14a) and Mobile Security (KA14b).

As seen in Table 3, educational cybersecurity environments outlined in these papers are primarily focused on one area (or correlated group of areas) rather than trying to be broad and diverse. Therefore, laboratory environments are focused on demonstrating the most common network-type attacks (e.g., [54,55]) or web application attacks (e.g., [56–58]). In contrast, the laboratory environment presented in this paper strives to cover as many cybersecurity areas as possible. Thus, using the CyBOK classification, Table 3 shows that this cybersecurity course has the most Knowledge Areas covered (14 KAs). Due to this fact, students who pass this course gain comprehensive knowledge of this industry field, enabling them to select aspects they find interesting for potential further specialization, which is not facilitated by other presented courses.

Table 3. Comparison of different cybersecurity courses and environments based on covered Knowledge Areas. (x marks that an area is covered).

Paper	KA1	KA2	KA3	KA4	KA5	KA6	KA7	KA8	KA9	KA10	KA11	KA12	KA13	KA14a	KA14b	KA15	KA16	KA17	KA18	KA19	Total
[59,60]			x		x	x	x			x			x				x				7
[61]					x	x	x			x			x	x			x				7
[62]									x												1
[63]					x	x	x			x			x				x				6
[55]					x	x	x			x			x	x			x				7
[64]							x		x			x		x		x					5
[65]							x		x				x								3
[66]										x			x	x		x	x				5
[67]										x							x				2
[68]														x							1
[69]									x											x	2
[54]									x								x				2
[70,71]									x												1
[72]									x											x	2
[73]					x	x	x			x							x				5
[74]																	x		x		2
[75]					x	x	x										x				4
[76]																				x	1
[77]					x	x	x			x			x			x	x				7
[56]													x	x		x					3
[57]													x	x		x					3
[78]													x	x		x					3
[79]													x	x		x					3
[80]									x					x							2
[81]																	x				1
[82]													x	x		x					3
[83]			x							x			x	x		x					5
[58]													x	x		x					3
[84]																	x				1
[85]					x	x	x										x				4
[86]					x	x	x		x	x			x	x			x				8
[87]									x	x			x	x			x				5
[88]					x	x	x			x			x	x			x				7
[89]										x			x	x			x				4
[90]														x			x				2
[91]																	x			x	2

Table 3. *Cont.*[illegible]

2.3. Comparison Based on Architecture and Deployment Technology

There have also been several attempts to classify educational laboratory environments for teaching cybersecurity. Classifications have been made upon the implementation target of laboratory exercises, whether it is due to physical or virtual machines/devices, e.g., where this can be conducted by using a desktop-based virtualization or cloud-based virtualization, as presented by a hierarchy in [22]), or in a simulated environment, as presented in [22]. The authors of [22] extract other characteristics of the environment:

- Remote access (C1);
- The need for lab scheduling (C2);
- Persistent storage (C3);
- Configuration level (C4).

Along with these characteristics, we propose several other characteristics that were extracted as crucial for the comparison of different cybersecurity laboratories because they help to show an even clearer picture of the modularity, usability, and details of the evaluation of a particular laboratory demonstrated in the research paper:

- Ability to share the laboratory (C5);
- The number of students/users used for the evaluation; sample sizes (C6);
- The maximum capacity of students (C7);
- The method of evaluation (C8);
- Implementation (C9).

In Table 4, a comparison of related papers is made based on the mentioned characteristics that describe a laboratory environment based on its architecture and deployment technology.

As seen by the overview shown in Table 4, most papers do not delve into the details of the implementation of the laboratory environment itself (e.g., [88,89]). This is because the papers usually focus more on the impact and broadening of cybersecurity knowledge that the environment and the course itself have on students. This paper, in contrast, focuses on showing the modularity of the laboratory environment and the implementation details that make the mentioned modularity possible. This takeaway can also be seen by analyzing other characteristics shown in the table. In contrast to different laboratory environments, which do not usually allow that much ease of use by analyzing the characteristics in the table, all the modularity and ease-of-use characteristics are true for the one presented in this paper.

Another characteristic that can be noted is that evaluation is conducted on a relatively small group of students (usually up to 50 students and a maximum of 147 students in the analyzed papers). The evaluation is also mostly conducted only using surveys (e.g., [87,90]). Therefore, this paper focuses on demonstrating the results of the cybersecurity course as thoroughly as possible, thus using a bigger group of students (313) to evaluate their experience by surveying them and analyzing their academic results.

From the table, it can be seen that almost 50% (18 laboratory environments) do not have the ability for remote access, while the ANS laboratory does. In addition, 10 laboratory environments clearly present the need for scheduling, while the ANS laboratory is flexible and allows students to access it whenever they desire.

Table 4. Comparison of different cybersecurity courses and environments based on covered Knowledge Areas (x—no information available).

Paper	C1	C2	C3	C4	C5	C6	C7	C8	C9
[59,60]	yes	no	yes	high	yes	27 in total	x	Surveys and Academic results	VMs
[61]	yes	no	yes	medium	yes	60 in total	90 students	Surveys	Physical Network
[62]	yes	no	yes	medium	no	28 in total	15 students at once	Surveys	Web application
[63]	no	yes	yes	medium	no	56 in total	9 computers	Surveys and competition scores	Physical Machines
[55]	yes	no	yes	x	yes	42 in total	Up to 1000 VMs	Surveys and Academic results	Server with VMs
[64]	yes	no	yes	high	no	64 in total	x	Surveys and Academic results	Software
[65]	no	yes	no	low	no	54 in total	20 laptops	Surveys	Physical Machines with VMs
[66]	no	no	yes	low	no	30 average	x	Surveys	VM
[67]	yes	no	yes	x	no	x	x	x	Physical Hardware
[68]	no	no	yes	x	no	40 in total	x	Surveys	Web Application
[69]	no	yes	no	low	no	x	x	Surveys	Physical Machines
[54]	no	no	no	low	no	109 in total	x	Surveys and Academic results	Desktop Application
[70,71]	no	yes	no	low	no	18 in total	x	Surveys and Academic results	Physical Machines
[72]	x	no	yes	low	no	x	x	Surveys	VMs
[73]	no	yes	no	low	no	x	15 desktops	Academic results	VMs
[74]	yes	no	no	high	no	x	x	Surveys and Academic results	Emulated environment
[75]	yes	no	yes	x	yes	104 students	x	Academic results	VMs on server
[76]	yes	no	no	x	no	x	x	x	Simulation Engine
[77]	yes	no	yes	low	no	x	x	x	Web Application
[56]	yes	no	yes	medium	yes	23 students	x	Surveys	Web Server
[57]	no	no	yes	x	no	117 students	x	Surveys	Web Application
[78]	yes	no	yes	x	no	x	x	x	VMs
[79]	no	no	yes	x	no	x	x	Student Feedback	Web Application
[80]	no	no	yes	x	no	122 students	x	Surveys and Academic results	VMs
[81]	no	x	x	medium	no	20 students	x	Surveys	VMs
[82]	yes	x	yes	high	yes	x	600 VMs used	x	VMs
[83]	yes	no	yes	x	x	19 students	x	Surveys	VMs
[58]	no	x	x	x	x	147 in total	x	Surveys	Web Applications Tool
[84]	no	x	x	x	no	47 in total	12 labs in total	Surveys	Emulated network
[85]	yes	x	yes	low	no	x	x	x	VMs
[86]	yes	no	yes	low	no	x	x	x	VMs
[87]	yes	no	yes	low	no	x	x	Surveys	VMs
[88]	yes	no	yes	high	yes	x	x	x	VMs
[89]	yes	no	yes	x	no	x	x	x	Software Platform
[90]	yes	no	yes	medium	yes	9 in total	x	Surveys	VMs on Cloud Servers
[91]	no	yes	no	medium	yes	20+ students	x	Surveys and Academic results	Software and RFID Reader

Table 4. Cont.

Paper	C1	C2	C3	C4	C5	C6	C7	C8	C9
[92]	no	yes	no	low	no	9 students	x	Surveys	Hardware and Software tools
[93]	no	no	yes	medium	no	16 students	x	Surveys	Software
[94]	no	yes	yes	high	yes	29 students	200+ students	Surveys	Physical Machines
[95]	yes	no	yes	high	no	15 learners	x	Surveys and Academic results	VMs
[96]	yes	no	yes	high	yes	76 students	x	Academic results	Hardware and VMs
[97]	yes	yes	yes	low	no	x	x	x	VMs
[98]	yes	yes	yes	medium	no	x	x	Surveys and Academic results	Hardware and Software
[99]	yes	no	yes	high	yes	25 students	x	Surveys and Academic results	VMs on Server
ANS course	yes	no	yes	high	yes	313 students total	84 concurrent laboratories	Surveys and Academic results	VMs on Servers

It can also be observed that many of the laboratory environments do not present a way of achieving a high configuration (therefore, many of the laboratory environments have a low configuration level). This is mostly due to the fact that the description presented in the paper either does not delve into the details of the configuration of the laboratory environment or the presented environments are described in such a way that they only fit into the mold of the already-mentioned set of exercises and therefore cannot be changed for any other. The ANS laboratory environment, due to its approach to design, where virtual machines were used to build it, allows expansion by installing any new scenario either on the existing virtual machines or by adding a new one to fit the purposes of the new exercise (the only criteria here is that there is storage for the new virtual machines). The details of the design and configurability of the laboratory environment will be expanded on in the following section.

3. Course Description

The ANS course is an elective course in master's degree studies in the Computer Engineering module. It introduces students to computer system and network security, intrusion and attack detection and prevention, and ethical hacking methodologies. The course aims to teach students to recognize key threats and attack vectors on computer and software systems through a series of practical laboratory exercises. The course consists of 2 h of theoretical lectures, 2 h of practical laboratory exercises, and 1 h of other classes per week. In the other types of classes, students prepare an essay paper on some recently discovered weaknesses and attack vectors.

The ANS course covers the following topics:

- Attacks on computer systems and networks (methodology and phases);
- Tools and methodologies for the reconnaissance, scanning, and enumeration of computer systems and network data (KA16),
- Social engineering (KA3, KA5, KA6);
- Network (IP, ARP, DNS, BGP, WiFi, Bluetooth) attacks and tools for system protection: access lists, firewalls, intrusion detection/prevention systems and methodologies, and honeypots (KA5, KA7, KA9, KA16, KA19);
- (Distributed) denial of service attacks and botnets (KA5, KA15, KA16);
- Malware (KA5);
- Web application attacks (SQLi, XSS) (KA13, KA14a, KA15);
- Gaining access, password guessing, operating system vulnerabilities, privilege escalation, and shellcoding. (KA3, KA6, KA10, KA12, KA13),
- Anonymity on the internet (KA9, KA19);
- Mobile device security (KA13, KA14b, KA15);
- Hardware security (KA17).

3.1. Laboratory Environment and Exercises

The ANS course includes more than 20 laboratory exercises spread across 13 topics. After the initial set of seven exercises developed in the ISSES project [4], the number of exercises has increased in each school year since the start of the course. Table 5 shows the set of topics covered by the laboratory exercises that were available on the ANS course in each of the school years so far.

The aim was to cover as many topics as possible with exercises that the students would manually perform following a guided tutorial. However, for some of them, like WiFi password cracking, there was not enough available equipment (access points) to allow all the students to perform them manually, so these were conducted as demonstrations, which were recorded and provided to students.

As shown in Table 5, the ANS course covers diverse topics often separated into different courses in other institutions. The key challenge in creating a laboratory environment for this course is enabling different lab exams to be executed on the same equipment. While for some laboratory exercises, a docker-based environment would be scalable and flexible (e.g., web application attacks), for network-based attacks (e.g., ARP spoofing, DNS poisoning), such an environment is insufficient, and at least a virtual network environment is needed. Further, the ANS course started in the spring semester of 2020. This was when the COVID-19 lockdown started, so another request was to enable the environment to be accessible to students remotely through a secure VPN connection, enabling working from home. This remained the practice after the lockdown period was over, as it offered the students flexibility to choose the time to perform the exercises. The laboratory is available to the students during the whole semester.

Table 5. The set of topics covered by the ANS course laboratory exercises. M denotes exercises that students perform manually, and D denotes exercises performed as a demonstration.

Lab Exercise	School Year			
	Y1	Y2	Y3	Y4
Packet analysis—Wireshark	M	M	M	M
Network scanning—nmap	M	M	M	M
ARP spoofing	M	M	M	M
DNS spoofing	M	M	M	M
IP filtering and Firewall	M	M	M	M
Web application attacks (XSS, SQLi)	M	M	M	M
WiFi password cracking	D	D	D	D
Reconnaissance—DNS, email, maltego		D	D	M
Hiding files		M	M	M
Password cracking—ophcrack and hashcat		M	M	M
Spyware		M	M	M
Privilege escalation, shellcoding (5 labs)		M	M	M
Erasing traces		M	M	M

The ANS laboratory was built on top of VMware vSphere’s virtualized environment. Two students receive their isolated share of resources, which consists of six virtual machines and a set of virtual network connections, as depicted in Figure 1. The laboratory environment was designed so that sharing a laboratory is possible without one student’s work interfering with the other’s. All network segments between the virtual machines (including those directly connecting VM1 and VM2, VM1 and VM4, and so on) are separated, and packets appearing in one segment are not visible in the other segments.

The virtual machines VM1, VM2, and VM3 have the latest version of Ubuntu installed, VM4 is a pfSense firewall, VM5 is a 32-bit Linux machine used for shellcoding privilege escalation exercise, and VM6 is a Windows 7 virtual machine used for spyware, password cracking, file hiding, and erasing traces exercises. Virtual machines 1–5 have one core and 1GB of RAM allocated, sufficient for all the exercises. Each lab is accessible through the OpenVPN server and has a connection to the internet. Such a topology, especially the full mesh of logically separated network connections between virtual machines 1–4, enables the creation of various cases and topologies needed to execute exercises, especially the network-related part of the exercises.

The laboratory consists of four ThinkSystem SR550 servers, Lenovo (Beijing, China) with Intel(R) Xeon(R) Gold 5120 processors with 56 cores, 256 GB RAM, and 3.5 TB disks each. These servers form a cluster powered by VMware ESXi, 8.0.3. One laboratory environment requires approximately 11 GB of RAM in a basic configuration, allowing 84 concurrent and fully isolated laboratories.

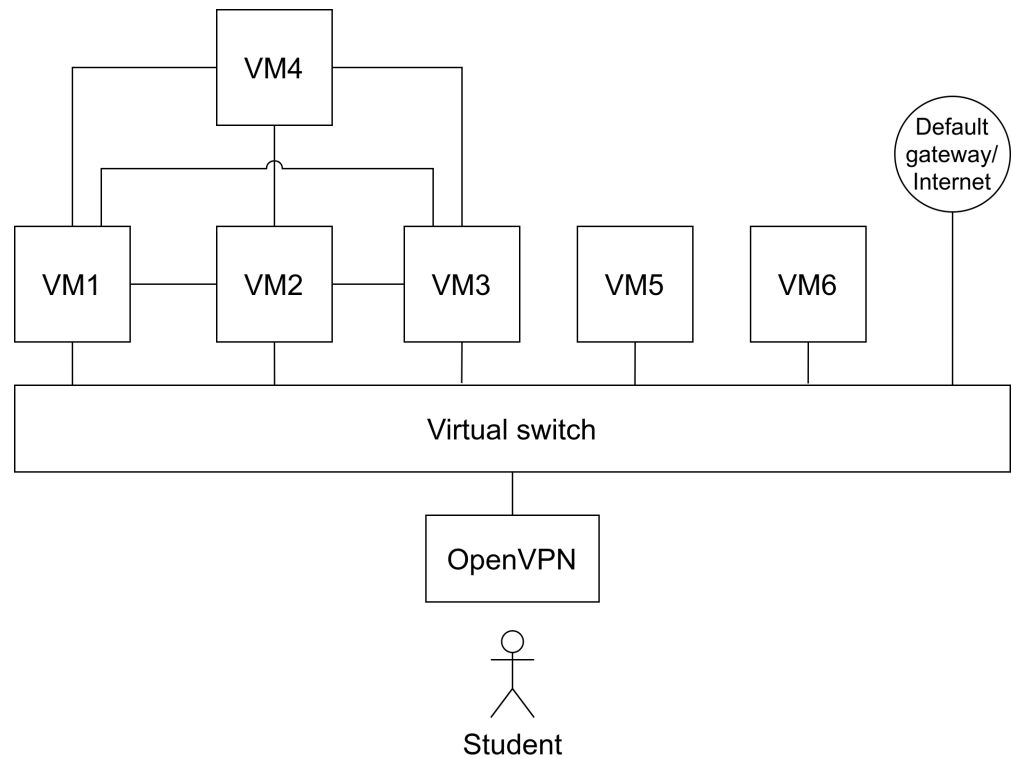


Figure 1. The logical topology of a student's lab environment.

Given the number of students that have taken the course (given in Section 4), creating an environment like this means several hundred virtual machines must be created. Since all the lab exercises in the course could be performed using the same lab setup created at the beginning of the semester, the laboratory configuration is static and does not have to be changed during the semester, although a change in configuration is possible. The only action needed is the restart of some virtual machines, which might become inaccessible when students make some configuration mistake. This can be conducted through the vSphere Client, which can access all the students' environments. A much larger task is configuring the virtual machines appropriately for all the exercises. This is conducted partially by providing students with a guided step-by-step tutorial in which they install some of the necessary components, partially using the Ansible automation system (Ansible: <https://www.ansible.com>, accessed on 31 October 2024).

A series of Ansible playbooks are created to make the appropriate network configuration in all isolated lab environments, install new software, verify the installation, and so on.

3.2. Examination in ANS Course

The final grade in the ANS course depends on an essay paper on a selected vulnerability or attack (20%), a practical skills test (40%), and a final exam (40%). The practical skills test is used to assess students' practical skills that have been previously trained through a set of laboratory exercises that are not graded by themselves. It combines red-team and capture-the-flag challenges in which each student is in a separate laboratory environment, a subset of the described laboratory environment configured with different

challenges. As an illustration, we describe the practical exam in the 2022/2023 school year examination period.

The topology is depicted in Figure 2. Each student received a description of the scenario. The only accessible machine at the beginning was the Attacker's machine. The goal was to gain access to the Administrator's machine using a series of steps taught in the laboratory exercises, which in that examination period were as follows:

- Discover the port and the address of the company web application.
- Find and exploit some of the vulnerabilities of the web server and discover the credentials on it.
- Access the web server and discover the administrator's address and credentials.
- Crack the password of the specific user on the web server.
- Gain access to the administrator's computer.
- Access the firewall and change its policy to allow later direct communication through the firewall.
- Erase all traces of the presence on all the machines touched.

The time for this open-book practical test was 2 h. To increase the practicality and applicability of knowledge from the practical test, scenarios were designed to include modern technologies that students would encounter in practice, for example, Spring Boot for the web server application.

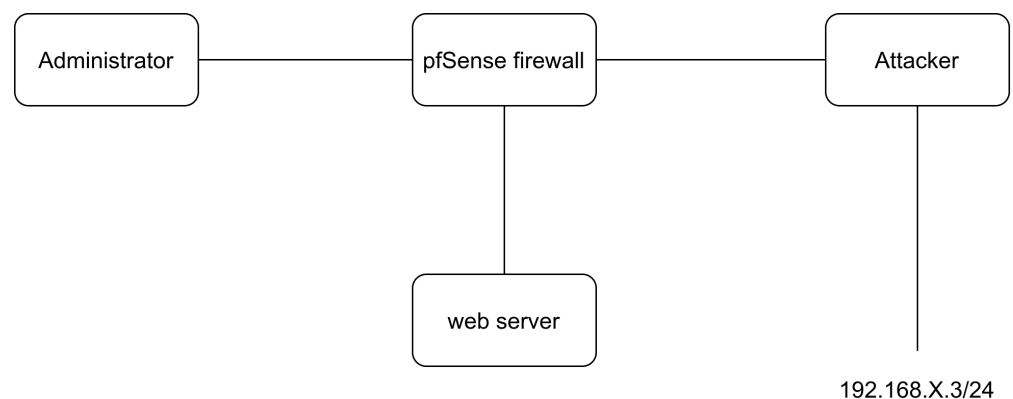


Figure 2. The logical topology of a student's lab environment.

4. Students' Practical Skills' Improvement Evaluation

The ANS course has been taught at SEE-UB since the 2019/2020 school year. In this section, we present the improvement of students' practical skills on the ANS course and how it affected their overall cybersecurity knowledge using quantitative and qualitative evaluation. Similar evaluation methods have been successfully used before, as in [100].

4.1. Quantitative Analysis

Quantitative analysis was performed based on data about students' achievement, which were collected in the analyzed period. To measure how the practical work on the course influenced students' practical skills' improvement, the following parameters were collected in each school year in which the course was taught (Y1, Y2, Y3, Y4):

- P1. The total number of students who took the course.
- P2. The percentage of students who passed the exam.
- P3. The percentage of students who did not take the final exam during a school year.
- P4. The total number of students who took the final exam at least once during a school year (active students).
- P5. The percentage of active students who passed the exam.

P6. The average grade for active students.

P7. The total number of students who achieved some points in the practical skills test.

P8. The average number of points in the practical skills test for students who achieved at least some points in the practical skills test.

P9. The percentage of active students who achieved some points in the practical skills test and successfully completed the exam.

P10. The average grade at the course for active students who achieved some points in the practical skills test.

Some students tried to complete the final exam more than once in a school year. For those students, their last attempt was calculated. The mentioned parameters are presented in Table 6.

Table 6. Statistics for the ANS course.

	Y1	Y2	Y3	Y4
P1	32	81	112	88
P2	75	70	55	53
P3	25	26	45	42
P4	24	60	62	51
P5	100	95	100	92
P6	9.04	8.48	9.06	7.98
P7	24	61	63	52
P8	38.29	31.53	34.17	26.12
P9	100	98	100	94.3
P10	9.04	8.65	9.06	8.04

Table 6 shows that after the initial introduction of the course in Y1, there was a significant increase in the number of students electing the course, which reached its maximum in Y3 but remained high in Y4 as well (P1).

It is important to note that during this period, the number of students enrolled in the Computer Engineering module was between 29 and 59, and many students enrolled in the Software Engineering module, who chose to study software-related topics at the master's degree level, also elected this course. Another piece of information important for the analysis of the results is that the number of students enrolled in the ANS course with a Computer Science background from the bachelor's level was between 27 and 104.

The next observation is that with the increase in the number of students who elected the course, there was a constant drop in the percentage of students who passed the exam (P2). When we investigated this fact further, we noticed that we also had a continuous increase in the percentage of students who elected the course but never took the final exam during the school year (P3), and in most cases, these students did not complete any component of the course. This is explained by the fact that many of the master's degree students at our institution are employed full-time in commercial companies where obtaining a master's degree does not bring any benefits, resulting in a significant number of student drop-outs.

In the remainder of our analysis, we focus on students who took the final exam at least once during the school year (P4). When we measured the percentage of students that passed the exam for this group of students (P5), we noticed much better results than before (P2), with the lowest achievement in Y4 at 92 percent and a 100 percent result two times (Y1 and Y3). The average grades for this group of students (P6) were between 7.98 and 9.06. To measure how laboratory exercises and practical skills tests influenced students' overall

success on the exam, we looked at how many students achieved at least some points on the practical skills test (P7). We noticed only a few students per school year who either achieved some points on the practical skills test but never took the final exam or did not achieve any points on the practical skills test but took the final exam. That is why the P7 metric is close to P4. This means that most of the students who took the final exam achieved at least some points on the practical skills test, and most of the students who achieved at least some points on the practical skills test also took the final exam. The average number of points for this group of students (P8) was between 26.12 and 38.22 (out of 40). Next, we measured the success of the exam for students who achieved at least some points on the practical skills test and took the final exam at least once during the school year (P9 and P10). When we compare this to P5 and P6, it can be observed that for Y1 and Y3, these parameters are the same, and for Y2 and Y4, P9 and P10 are slightly better.

To confirm the hypothesis that the practical skills component was significant for students' overall success, we used Spearman's rank correlation between the points won on the practical skills test and the final grade for each school year. For this reason, we collected an additional parameter:

P11. Spearman's rank correlation (R /two-tailed p) between the points won in the practical skills test and the final grade (active students) for students who achieved some points in the practical skills test.

Table 7 shows these results.

Table 7. Additional statistics for the ANS course.

	Y1	Y2	Y3	Y4
P11	$rs = 0.4201; p$ (2-tailed) = 0.04094	$rs = 0.6837; p$ (2-tailed) = 0	$rs = 0.7385; p$ (2-tailed) = 0	$rs = 0.8587; p$ (2-tailed) = 0

The results from Table 7 show that the association between those two variables could be considered statistically significant.

To test the validity of the quantitative analysis, we used two-way ANOVA. For this reason, additional parameters were collected:

P12. The average number of points in the final exam and essay paper for students who achieved some points in the practical skills test.

P13. The average number of points in the final exam and essay paper for students who achieved 0 points in the practical skills test but achieved a total sum of points greater than 0.

Table 8 shows these statistics.

Table 8. Additional statistics for the ANS course.

	Y1	Y2	Y3	Y4
P11	46.82	46.73	49.87	46.45
P12	NA	28.58	19.23	21.2

The first factor in the analysis was the group of students and the second factor was the school year. Students were grouped in two groups based on their completion of the practical skills test. The dependent variable was the average number of points in the final exam and the essay paper. In Y1, all students who achieved a total sum of points greater than 0 also achieved at least some points in the practical skills test, and that is why the P13 parameter was NA. Y1 was excluded from the calculation of the two-way ANOVA test because P13 was NA and could not be taken into account during the calculation. For the first factor, the result

is significant $F(1,203) = 196.3369$; $p = 0$. For the second factor, the result is also significant $F(2,203) = 3.387$; $p = 0.03573$. On the other hand, the interaction between the analyzed factors is not significant $F(2,203) = 0.8032$; $p = 0.4493$. These results prove that improving practical skills in the ANS laboratory resulted in the overall improvement of the gained knowledge and also explain variations in the P6 parameter during the analyzed period.

4.2. Qualitative Analysis

To obtain students' feedback on the course's organization and associated laboratory environment and exercises, two surveys were conducted: the first was on students who elected the course (S1), and the second was on students who took the practical skills test (S2). The surveys were conducted in four consecutive school years (2019/2020, 2020/2021, 2021/2022, and 2022/2023). They were anonymous and voluntary, with Google Forms being used to implement the surveys. A total of 62 students took the S1 survey, and 73 took the S2 survey. Both surveys consisted of the Likert scale and open-ended questions, while the S2 survey also had interval scale questions, as suggested in [101].

4.2.1. S1 Survey Results

In the first survey, the Likert scale statements were as follows: S1LS1. The technologies used in the practical part of the course were easy to understand. S1LS2. The organization of the course was satisfying. S1LS3. The organization of the practical part of the course was satisfying. S1LS4. Overall experience at the course was positive. Students could choose one of five answers: SA—strongly agree; A—agree; NAND—not agree not disagree; D—disagree; and SD—strongly disagree. Figure 3 presents the results of the S1 survey. The answers are grouped in the following manner: agree (A and SA), neutral (NAND), disagree (D and SD). Their percentage for each school year is shown.

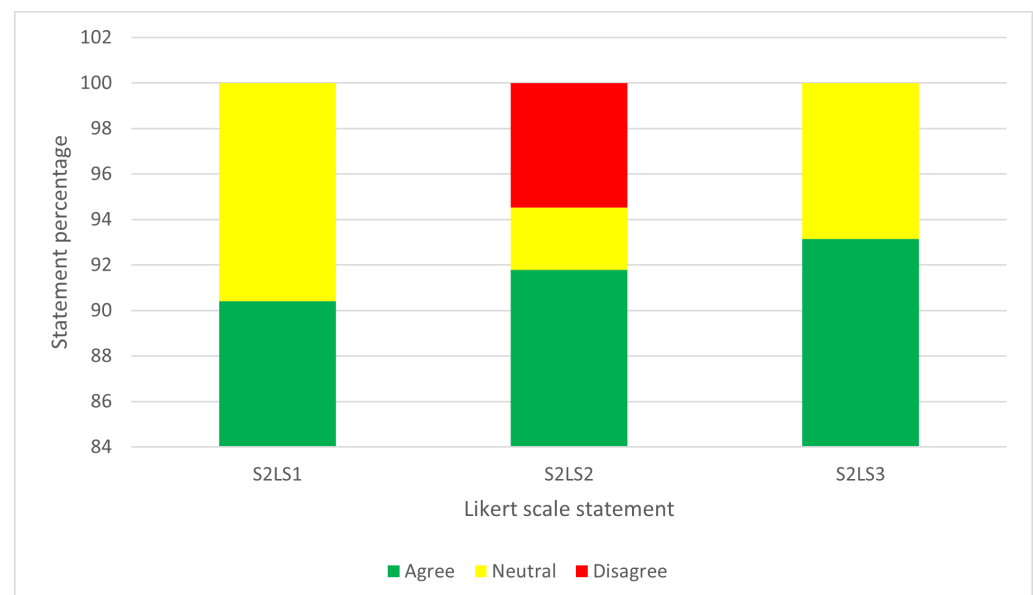


Figure 3. Results of S1 survey.

Around 77% of students thought that it was easy to understand the technologies used in the practical part of the course (S1LS1). Approximately 87% of students were satisfied with the course's organization (S1LS2). However, only around 81% were satisfied with the organization of the practical part of the course (S1LS3), with the highest percentage of disagreement (around 11%). Overall, students were satisfied with the course (S1LS4), with over 93% of them agreeing and none of them disagreeing. To understand the reasons for

the lower satisfaction with the practical part of the course, we investigated the answers to S1LS3 question thoroughly, as presented in Table 9.

Table 9. Absolute number of student answers to S1LS3 question divided by school years.

S1LS3	SD (1)	D (2)	NAND (3)	A (4)	SA (5)	Average
Y1	0	1	1	3	5	4.2
Y2	1	3	1	7	13	4.12
Y3	0	1	3	5	7	4.13
Y4	1	0	0	5	5	4.18
Total	2	5	5	20	30	4.14

Table 9 shows that student satisfaction with the practical part of the course was similar throughout the years, and in total, it was high, with an average of 4.14 out of 5. To understand the reasons why this question was graded a bit lower than the other questions, we analyzed the answers to the open-ended questions, the results of which are given below. In the S1 survey, the open-ended questions were as follows: S1OE1. Name the most interesting and the least interesting topic in the course. S1OE2. Name the most interesting and the least interesting topic in the practical part of the course. S1OE3. Name the biggest pros and cons regarding the course.

For the S1OE1 question in all school years, almost all topics were mentioned as the most interesting, but most of them were also mentioned as the least interesting topics. On the other hand, for the S1OE2 question, most students agreed that SQLi, XSS, and DNS spoofing were the most interesting topics, while IP spoofing, firewall, and Wireshark were the least interesting topics. Regarding the biggest cons, the students mostly mentioned the high volume of the topics covered in the course and some technical issues with the usage of the laboratory (e.g., the VPN not working or access to some VM not being possible). Regarding the pros, they agreed that the topics were very interesting and up-to-date and that the practical work of the course was realistic and useful (S1OE3).

4.2.2. S2 Survey Results

In the second survey, the first interval scale question (S2IS1) was used to find out how much time the students needed to prepare for the practical skills test. The answers were provided in intervals of 8 h (one working day). Figure 4 shows the results obtained for each school year. More than 92% of students completed the preparation for all school years in not more than four days. The results showed that the difficulty of the practical skills test was well estimated.

Another interval scale question (S2IS2) was used to find how many laboratory exercises students were able to complete successfully. The answers were provided in intervals of 10 percent. Figure 5 shows the results obtained for each school year. More than 87% of students completed more than 80% of the laboratory exercises for all school years.

The S2 Likert scale statements were as follows: S2LS1. The practical skills test helped me to better understand the course material. S2LS2. The laboratory exercises helped me to prepare for the practical skills test. S2LS3. Overall experience with the practical skills test was positive. The scale items were the same as in the S1 survey, and results were gathered and analyzed the same way as in the S1 survey. Table 10 presents the results of the S2 survey. The answers are grouped in the same manner as for the S1 survey analysis, but this time, they are aggregated for all four school years.

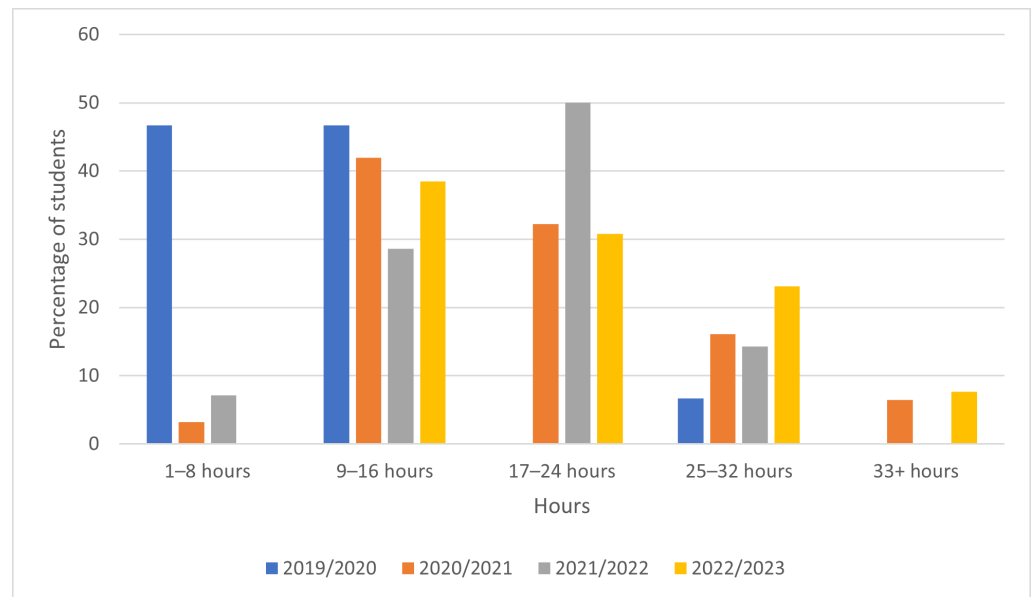


Figure 4. Number of hours needed for preparation for practical skills test.

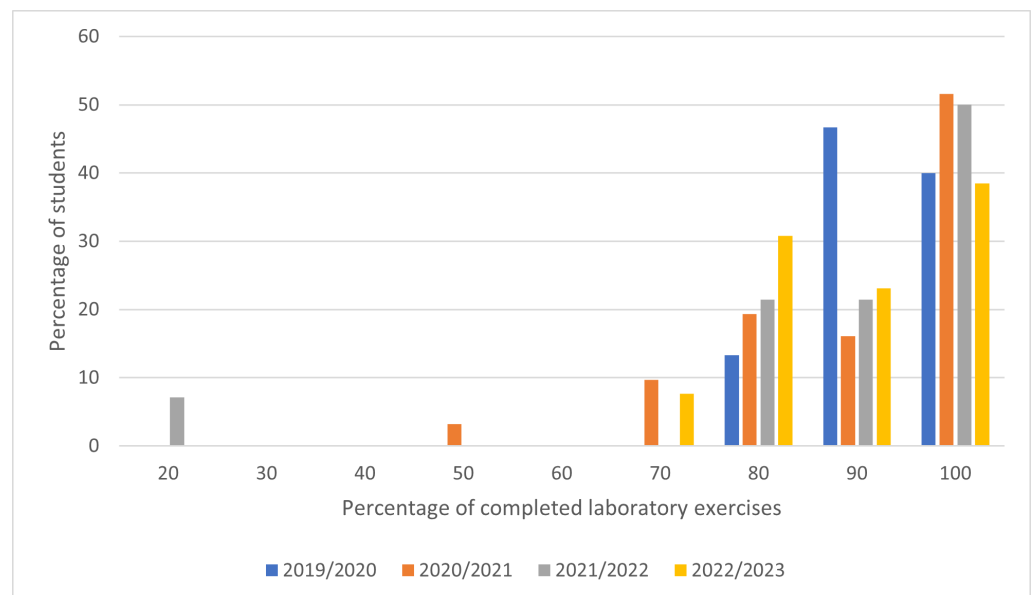


Figure 5. Percentage of laboratory exercises that students completed.

Table 10. Results of S2 survey.

	Agree	Neutral	Disagree
S2LS1	90.41	9.59	0
S2LS2	91.78	2.74	5.48
S2LS3	93.15	6.85	0

According to more than 90% of students, the practical skills test helped with the understanding of the course material (S2LS1). Similarly, the laboratory exercises helped approximately 92% of students prepare for the practical skills test (S2LS2). Overall, students were satisfied with the practical skills test (S2LS3), with over 93% of them agreeing and none of them disagreeing.

In the S2 survey, the open-ended questions were as follows: S2OE1. Should anything be changed in the organization of the practical skills test? S2OE2. Name the biggest pros and cons regarding the practical skills test.

For the S2OE1 question, most students who gave their answer replied that nothing should be changed, and only some students suggested that the test should last 30 min longer. Regarding the biggest cons, the students mostly had no complaints, and only a few complained about some technical issues they experienced with the laboratory environment. Regarding pros, they agreed that it helped them understand the course material through practical examples and that it was very interesting for them (S2OE2).

5. Conclusions

In this paper, a novel ANS course and the laboratory environment used in the course were presented. A thorough review was made that led to the comparison of the described course to 44 other related courses based on the coverage of the topics according to CyBOK classification and on the development characteristics of the laboratory environment. It was shown that the ANS course covers a broader scope of topics compared to other related courses. The laboratory environment described is flexible and multidisciplinary in the sense that it covers different types of laboratory exercises, can easily add new laboratory exercises, scales well to increase the number of students, and enables students to work from home. The practical skills test allows students to express their creativity in a real-world situation, shown through the correlation between the practical test results and their final grade and general results in the course and the positive feedback for the practical part of the course. Finally, the laboratory environment enables students to perform their master's thesis research on topics not already covered through laboratory exercises.

Because of constantly changing attack vectors and the number of various examples of cyber attacks that appear daily, the key challenge for the ANS course is to balance the course relevance through the chosen set of covered topics, practical exercises, and demonstrations on one side and to keep the total amount of work manageable during the semester. There are plans to add laboratory exercises that broaden the topic of Web Security (e.g., with exercises that demonstrate CSRF attacks) as well as Mobile Security to demonstrate a couple of different attacks on Android devices, as was proposed in [102].

Author Contributions: Conceptualization, P.V. and Ž.S.; Methodology, M.O., P.V. and Ž.S.; Validation, P.V.; Investigation, M.O., P.V. and Ž.S.; Data curation, M.O. and Ž.S.; Writing—original draft, M.O., P.V. and Ž.S.; Writing—review & editing, M.O., P.V. and Ž.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was financially supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, contract number: 451-03-65/2024-03/200103.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Morgan, S. Global Ransomware Damage Costs Predicted to Exceed \$265 Billion by 2031. Available online: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/> (accessed on 8 March 2024).
2. ISC2 Cybersecurity Workforce Study, 2023. Available online: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf (accessed on 8 March 2024).
3. Erasmus Capacity Building in Higher Education Program. Available online: https://erasmus-plus.ec.europa.eu/opportunities/opportunities-for-organisations/cooperation-among-organisations-and-institutions/capacity-building-higher-education?facets__field_eac_tags=174 (accessed on 8 March 2024).
4. ISSES. Available online: <https://isses.etf.bg.ac.rs/> (accessed on 21 February 2024).
5. Certified Ethical Hacker. Available online: <https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/> (accessed on 8 March 2024).

6. Amo, L.C.; Liao, R.; Frank, E.; Rao, H.R.; Upadhyaya, S. Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Trans. Educ.* **2019**, *62*, 134–140. [\[CrossRef\]](#)
7. Childers, G.; Linsky, C.L.; Payne, B.; Byers, J.; Baker, D. K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Comput. Educ. Open* **2023**, *4*, 100119. [\[CrossRef\]](#)
8. Raja, A.; Galvan, J.; Li, Y.; Yuan, J. UCLP: A Novel UAV Cybersecurity Laboratory Platform. In Proceedings of the 22nd Annual Conference on Information Technology Education, SnowBird, UT, USA, 6–9 October 2021; pp. 23–28. [\[CrossRef\]](#)
9. Frontera, P.J.; Rodríguez-Seda, E.J. Network Attacks on Cyber-Physical Systems Project-Based Learning Activity. *IEEE Trans. Educ.* **2021**, *64*, 110–116. [\[CrossRef\]](#)
10. Balon, T.; Baggili, I.A. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Educ. Inf. Technol.* **2023**, *28*, 11759–11791. [\[CrossRef\]](#) [\[PubMed\]](#)
11. Bendler, D.; Felderer, M. Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM Trans. Comput. Educ.* **2023**, *23*, 1–33. [\[CrossRef\]](#)
12. Beuran, R.; Vykopal, J.; Belajová, D.; Čeleda, P.; Tan, Y.; Shinoda, Y. Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms. *Comput. Secur.* **2023**, *128*, 103120. [\[CrossRef\]](#)
13. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Comput. Secur.* **2018**, *75*, 24–35. [\[CrossRef\]](#)
14. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber Ranges and TestBeds for Education, Training, and Research. *Appl. Sci.* **2021**, *11*, 1809. [\[CrossRef\]](#)
15. Ebad, S.A.; Ebad, C.A.S. What topics should or should not be included in software security education—Qualitative content analysis. *Comput. Appl. Eng. Educ.* **2022**, *30*, 1753–1773. [\[CrossRef\]](#)
16. González-Manzano, L.; de Fuentes, J.M. Design recommendations for online cybersecurity courses. *Comput. Secur.* **2019**, *80*, 238–256. [\[CrossRef\]](#)
17. Pittman, J. Understanding System Utilization as a Limitation Associated with Cybersecurity Laboratories—A Literature Analysis. *J. Inf. Technol. Educ. Res.* **2013**, *12*, 363–378. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Prvan, M.; Ožegović, J. Methods in Teaching Computer Networks: A Literature Review. *ACM Trans. Comput. Educ.* **2020**, *20*, 1–35. [\[CrossRef\]](#)
19. Rashid, A.; Danezis, G.; Chivers, H.; Lupu, E.; Martin, A.; Lewis, M.; Peersman, C. Scoping the Cyber Security Body of Knowledge. *IEEE Secur. Priv.* **2018**, *16*, 96–102. [\[CrossRef\]](#)
20. Saharinen, K.; Backlund, J.; Nevala, J. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. In Proceedings of the 12th International Conference on Education Technology and Computers, London, UK, 23–26 October 2020; pp. 172–176. [\[CrossRef\]](#)
21. Švábenský, V.; Vykopal, J.; Čeleda, P. What Are Cyber-security Education Papers About? A Systematic Literature Review of SIGCSE and ITICSE Conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education, Portland, OR, USA, 11–14 March 2020; Volume 7. [\[CrossRef\]](#)
22. Topham, L.; Kifayat, K.; Younis, Y.; Shi, Q.; Askwith, B. Cyber Security Teaching and Learning Laboratories: A Survey. *Inf. Secur. Int. J.* **2016**, *35*, 51–80. [\[CrossRef\]](#)
23. Ukwandu, E.; Farah, M.A.B.; Hindy, H.; Brosset, D.; Kavallieros, D.; Atkinson, R.; Tachtatzis, C.; Bures, M.; Andonovic, I.; Bellekens, X. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensor* **2020**, *20*, 7148. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Yamin, M.M.; Katt, B.; Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Comput. Secur.* **2020**, *88*, 101636. [\[CrossRef\]](#)
25. Zhang, R.I.; Xu, C.; Xie, M. Powering hands-on cybersecurity practices with cloud computing. In Proceedings of the Proceedings—International Conference on Network Protocols, ICNP, Chicago, IL, USA, 8–10 October 2019. [\[CrossRef\]](#)
26. Battisti, F.; Boato, G.; Carli, M.; Neri, A. Teaching multimedia data protection through an international online competition. *IEEE Trans. Educ.* **2011**, *54*, 381–386. [\[CrossRef\]](#)
27. Gerontakis, G.; Voyiatzis, I.; Yannakopoulos, P. Security Operations Center in Education: Building an Educational Environment for Attack and Defense Scenarios. In Proceedings of the 26th Pan-Hellenic Conference on Informatics, Athens Greece, 25–27 November 2022; pp. 27–31. [\[CrossRef\]](#)
28. Gkioulos, V.; Chowdhury, N. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 100361. [\[CrossRef\]](#)
29. Samonte, M.C.J.; Baganay, K.U.N.; Fernandez, K.E.; Jamena, J.D.N. CyLearn: An Assistive Web-Based e-Learning System for Cybersecurity Skills Course. *Int. J. Inf. Educ. Technol.* **2023**, *13*, 932–941. [\[CrossRef\]](#)
30. Saglam, R.B.; Miller, V.; Franqueira, V.N. A Systematic Literature Review on Cyber Security Education for Children. *IEEE Trans. Educ.* **2023**, *66*, 274–286. [\[CrossRef\]](#)
31. Zhang-Kennedy, L.; Chiasson, S. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.* **2022**, *54*, 1–39. [\[CrossRef\]](#)

32. Ahmed, A.; Lundqvist, K.; Watterson, C.; Baghaei, N. Teaching Cyber-Security for Distance Learners: A Reflective Study. In Proceedings of the Proceedings—Frontiers in Education Conference, FIE, Uppsala, Sweden, 21–24 October 2020. [\[CrossRef\]](#)
33. Akgul, A.; Kacar, S.; Pehlivan, I.; Aricioglu, B. Chaos-based encryption of multimedia data and design of security analysis interface as an educational tool. *Comput. Appl. Eng. Educ.* **2018**, *26*, 1336–1349. [\[CrossRef\]](#)
34. Beuran, R.; ichi Chinen, K.; Tan, Y.; Shinoda, Y. Towards effective cybersecurity education and training. *Res. Rep.* **2016**, *IS-RR-2016-003*, 1–16.
35. Daniel, C.; Mullarkey, M.; Agrawal, M. RQ Labs: A Cybersecurity Workforce Talent Program Design. *Commun. Comput. Inf. Sci.* **2022**, *1549 CCIS*, 171–185. [\[CrossRef\]](#)
36. Deng, Y.; Lu, D.; Huang, D.; Chung, C.J.; Lin, F. Knowledge Graph based Learning Guidance for Cybersecurity Hands-on Labs. In Proceedings of the ACM Conference on Global Computing Education, Chengdu, China, 17–19 May 2019; pp. 194–200. [\[CrossRef\]](#)
37. Floyd, B.; Jackson, J.; Probst, E.; Liu, H.; Mishra, N.; Zhong, C. Understanding Learners’ Interests in Cybersecurity Competitions on Reddit. In Proceedings of the 13th International Conference on Education Technology and Computers, Wuhan China, 22–25 October 2021; pp. 444–449. [\[CrossRef\]](#)
38. Hamman, S.T.; Hopkinson, K.M.; Markham, R.L.; Chaplik, A.M.; Metzler, G.E. Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students. *IEEE Trans. Educ.* **2017**, *60*, 205–211. [\[CrossRef\]](#)
39. Huang, H.J. Virtual Machine Software in Computer Network Security Teaching. *Adv. Intell. Syst. Comput.* **2021**, *1282*, 823–829. [\[CrossRef\]](#)
40. Kim, E.; Beuran, R. On designing a cybersecurity educational program for higher education. In Proceedings of the 10th International Conference on Education Technology and Computers, Tokyo, Japan, 26–28 October 2018; pp. 195–200. [\[CrossRef\]](#)
41. Koutchme, C.; Tilanterä, A.; Peltonen, A.; Hellas, A.; Haaranen, L. Exploring How Students Solve Open-ended Assignments: A Study of SQL Injection Attempts in a Cybersecurity Course. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education, Dublin, Ireland, 8–13 July 2022; pp. 75–81. [\[CrossRef\]](#)
42. Parekh, G.; Delatte, D.; Herman, G.L.; Oliva, L.; Phatak, D.; Scheponik, T.; Sharman, A.T. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Trans. Educ.* **2018**, *61*, 11–20. [\[CrossRef\]](#)
43. Shaorong, W.; Guiling, L. Research on campus network security protection system framework based on cloud data and intrusion detection algorithm. *Soft Comput.* **2023**, *27*, 6835–6844. [\[CrossRef\]](#)
44. Shillair, R.; Esteve-González, P.; Dutton, W.H.; Creese, S.; Nagyfejeo, E.; von Solms, B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Comput. Secur.* **2022**, *119*, 102756. [\[CrossRef\]](#)
45. Sun, J. Multi-dimensional alignment between online instruction and course technology: A learner-centered perspective. *Comput. Educ.* **2016**, *101*, 102–114. [\[CrossRef\]](#)
46. Tian, H. Comparative and Development of Network Information Teaching and Traditional Teaching Methods. In Proceedings of the 2021 4th International Conference on Information Systems and Computer Aided Education, 24–26 September 2021; pp. 1289–1293. [\[CrossRef\]](#)
47. Tsai, C.Y.; Shih, W.L.; Hsieh, F.P.; Chen, Y.A.; Lin, C.L.; Wu, H.J. Using the ARCS model to improve undergraduates’ perceived information security protection motivation and behavior. *Comput. Educ.* **2022**, *181*, 104449. [\[CrossRef\]](#)
48. Wang, L.; Tian, Z.; Gu, Z.; Lu, H. Crowdsourcing approach for developing hands-on experiments in cybersecurity education. *IEEE Access* **2019**, *7*, 169066–169072. [\[CrossRef\]](#)
49. Workman, M.D.; Luevanos, J.A.; Mai, B. A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model. *IEEE Trans. Educ.* **2022**, *65*, 40–45. [\[CrossRef\]](#)
50. Yamin, M.M.; Katt, B. Modeling and executing cyber security exercise scenarios in cyber ranges. *Comput. Secur.* **2022**, *116*, 102635. [\[CrossRef\]](#)
51. Zheng, W.; Feng, L.; Liu, B.; Fu, P.; Qiao, J. Development of virtual laboratory application structure in Android cellphone for distance learning. In Proceedings of the 1st International Conference on Electronics Instrumentation and Information Systems, EIIS 2017, Harbin, China, 3–5 June 2017; pp. 1–5. [\[CrossRef\]](#)
52. Zseby, T.; Vazquez, F.I.; King, A.; Claffy, K.C. Teaching Network Security with IP Darkspace Data. *IEEE Trans. Educ.* **2016**, *59*, 1–7. [\[CrossRef\]](#)
53. Cybersecurity Curricula 2017. Available online: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf (accessed on 5 March 2024).
54. Nielson, S.J. PLAYGROUND: preparing students for the cyber battleground. *Comput. Sci. Educ.* **2016**, *26*, 255–276. [\[CrossRef\]](#)
55. Xu, L.; Huang, D.; Tsai, W.T. Cloud-based virtual laboratory for network security education. *IEEE Trans. Educ.* **2014**, *57*, 145–150. [\[CrossRef\]](#)
56. Hendawi, A.; Basit, N.; Chen, J.; Sun, A. A Learning Platform for SQL Injection. In Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA, 27 February–2 March 2019; pp. 184–190. [\[CrossRef\]](#)

57. Ping, C.; Jinshuang, W.; Lanjuan, Y.; Lin, P. SQL Injection Teaching Based on SQLi-labs. In Proceedings of 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education, ICISCAE 2020, Dalian, China, 27–29 September 2020; pp. 191–195. [\[CrossRef\]](#)
58. Shar, L.K.; Poskitt, C.M.; Shim, K.J.; Wong, L.Y.L. XSS for the Masses: Integrating Security in a Web Programming Course using a Security Scanner. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education, Dublin, Ireland, 8–13 July 2022; pp. 463–469. [\[CrossRef\]](#)
59. Marsá-Maestre, I.; Hoz, E.D.L.; Giménez-Guzman, J.M.; López-Carmona, M.A. Using a scenario generation framework for education on system and internet security. In Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON), Marrakech, Morocco, 17–20 April 2012. [\[CrossRef\]](#)
60. Marsa-Maestre, I.; Hoz, E.D.L.; Gimenez-Guzman, J.M.; Lopez-Carmona, M.A. Design and evaluation of a learning environment to effectively provide network security skills. *Comput. Educ.* **2013**, *69*, 225–236. [\[CrossRef\]](#)
61. Abler, R.T.; Contis, D.; Grizzard, J.B.; Owen, H.L. Georgia Tech information security center hands-on network security laboratory. *IEEE Trans. Educ.* **2006**, *49*, 82–87. [\[CrossRef\]](#)
62. Ferreres, A.I.G.T.; Wouters, K.; Álvarez, B.R.; Garnacho, A.R. EVAWEB: A web-based assessment system to learn X.509/PKIX-based digital signatures. *IEEE Trans. Educ.* **2007**, *50*, 112–117. [\[CrossRef\]](#)
63. Lee, C.P.; Uluagac, A.S.; Fairbanks, K.D.; Copeland, J.A. The design of NetSecLab: A small competition-based network security lab. *IEEE Trans. Educ.* **2011**, *54*, 149–155. [\[CrossRef\]](#)
64. Luburić, N.; Sladić, G.; Slivka, J.; Milosavljević, B. A Framework for Teaching Security Design Analysis Using Case Studies and the Hybrid Flipped Classroom. *ACM Trans. Comput. Educ.* **2019**, *19*, 1–19. [\[CrossRef\]](#)
65. Wagner, P.J.; Phillips, A.T. A portable computer security workshop. *J. Educ. Resour. Comput. (JERIC)* **2006**, *6*, 3-es. [\[CrossRef\]](#)
66. Du, W.; Wang, R. SEED: A Suite of Instructional Laboratories for Computer Security Education. *J. Educ. Resour. Comput. (JERIC)* **2008**, *8*, 1–24. [\[CrossRef\]](#)
67. Stojanov, Z.; Dobrilovic, D.; Zorić, T. Exploring students' experiences in using a physical laboratory for computer networks and data security. *Comput. Appl. Eng. Educ.* **2017**, *25*, 290–303. [\[CrossRef\]](#)
68. Asghar, H.; Anwar, Z.; Latif, K. A deliberately insecure RDF-based Semantic Web application framework for teaching SPARQL/SPARUL injection attacks and defense mechanisms. *Comput. Secur.* **2016**, *58*, 63–82. [\[CrossRef\]](#)
69. Trabelsi, Z. Teaching network covert channels using a hands-on approach. In Proceedings of the IEEE Global Engineering Education Conference, EDUCON, Porto, Portugal, 27–30 April 2020; pp. 323–328. [\[CrossRef\]](#)
70. Stanisavljevic, Z.; Stanisavljevic, J.; Vuletic, P.; Jovanovic, Z. COALA—System for visual representation of cryptography algorithms. *IEEE Trans. Learn. Technol.* **2014**, *7*, 178–190. [\[CrossRef\]](#)
71. Stanisavljevic, Z.; Vuletic, P. Adding practical experience to computer security course. *Comput. Appl. Eng. Educ.* **2018**, *26*, 384–392. [\[CrossRef\]](#)
72. Zseby, T.; Vazquez, F.I.; Bernhardt, V.; Frkat, D.; Annessi, R. A Network Steganography Lab on Detecting TCP/IP Covert Channels. *IEEE Trans. Educ.* **2016**, *59*, 224–232. [\[CrossRef\]](#)
73. Othmane, L.B.; Bhuse, V.; Lilien, L.T. Incorporating lab experience into computer security courses. In Proceedings of the 2013 World Congress on Computer and Information Technology, WCCIT 2013, Sousse, Tunisia, 22–24 June 2013. [\[CrossRef\]](#)
74. Cruz, T.; Simões, P. Down the Rabbit Hole: Fostering Active Learning through Guided Exploration of a SCADA Cyber Range. *Appl. Sci.* **2021**, *11*, 9509. [\[CrossRef\]](#)
75. Zeng, Z.; Deng, Y.; Hsiao, I.; Huang, D.; Chung, C.J. Improving student learning performance in a virtual hands-on lab system in cybersecurity education. In Proceedings of the Proceedings—Frontiers in Education Conference, FIE, San Jose, CA, USA, 3–6 October 2018. [\[CrossRef\]](#)
76. Skracic, K.; Petrovic, J.; Pale, P.; Tralic, D. Virtual wireless penetration testing laboratory model. In Proceedings of the Proceedings Elmar—International Symposium Electronics in Marine, Zadar, Croatia, 10–12 September 2014; pp. 281–284. [\[CrossRef\]](#)
77. Tateiwa, Y. LiNeS Cloud: A Web-Based Hands-On System for Network Security Classes with Intuitive and Seamless Operability and Light-Weight Responsiveness. *IEICE Trans. Inf. Syst.* **2022**, *E105D*, 1557–1567. [\[CrossRef\]](#)
78. Zeng, H. Research on developing an attack and defense lab environment for cross site scripting education in higher vocational colleges. In Proceedings of the Proceedings—2013 International Conference on Computational and Information Sciences, ICCIS 2013, Shiyang, China, 21–23 June 2013; pp. 1971–1974. [\[CrossRef\]](#)
79. Uskov, A.V. Hands-on teaching of software and web applications security. In Proceedings of the 3rd Interdisciplinary Engineering Design Education Conference, IEDEC 2013, Santa Clara, CA, USA, 4–5 March 2013; pp. 71–78. [\[CrossRef\]](#)
80. Chen, L.C.; Tao, L. Teaching web security using portable virtual labs. In Proceedings of the 2011 11th IEEE International Conference on Advanced Learning Technologies, ICALT 2011, Athens, GE, USA, 6–8 July 2011; pp. 491–495. [\[CrossRef\]](#)
81. Fuertes, W.; Tunala, A.; Moncayo, R.; Meneses, F.; Toulkeridis, T. Software-Based Platform for Education and Training of DDOS Attacks Using Virtual Networks. In Proceedings of the Proceedings—2017 International Conference on Software Security and Assurance, ICSSA 2017, Altoona, PA, USA, 24–25 July 2017; pp. 94–99. [\[CrossRef\]](#)

82. Beuran, R.; Tang, D.; Pham, C.; ichi Chinen, K.; Tan, Y.; Shinoda, Y. Integrated framework for hands-on cybersecurity training: CyTrONE. *Comput. Secur.* **2018**, *78*, 43–59. [\[CrossRef\]](#)
83. Srivatanakul, T.; Annansingh, F. Incorporating active learning activities to the design and development of an undergraduate software and web security course. *J. Comput. Educ.* **2022**, *9*, 25–50. [\[CrossRef\]](#)
84. Wang, Z.; Guo, J. A Journey from End Systems to Backbone Routers: A Virtual Lab Environment for Online Computer Networking Courses. In Proceedings of the ASEE Conferences, Fayetteville, AR, USA, 26–29 July 2021. [\[CrossRef\]](#)
85. Lewis, J.; Lunsford, P. TLS man-in-the-middle laboratory exercise for network security education. In Proceedings of the 2010 ACM Conference on Information Technology Education, Midland, MI, USA, 7–9 October 2010; pp. 117–120. [\[CrossRef\]](#)
86. Wang, Y.; McCoey, M.; Hu, Q. Developing an Undergraduate Course Curriculum for Ethical Hacking. In Proceedings of the 21st Annual Conference on Information Technology Education, Virtual Event, 7–9 October 2020; pp. 330–335. [\[CrossRef\]](#)
87. Wang, Y.; McCoey, M.; Zou, H. Developing an Undergraduate Course Curriculum on Information Security. In Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 October 2018; pp. 66–71. [\[CrossRef\]](#)
88. Mirkovic, J.; Benzel, T. Teaching cybersecurity with DeterLab. *IEEE Secur. Priv.* **2012**, *10*, 73–76. [\[CrossRef\]](#)
89. Furfaro, A.; Piccolo, A.; Parise, A.; Argento, L.; Saccà, D. A Cloud-based platform for the emulation of complex cybersecurity scenarios. *Future Gener. Comput. Syst.* **2018**, *89*, 791–803. [\[CrossRef\]](#)
90. Li, Y.; Nguyen, D.; Xie, M. Ezsetup: A novel tool for cybersecurity practices utilizing cloud resources. In Proceedings of the 18th Annual Conference on Information Technology Education, Rochester, NY, USA, 4–7 October 2017; pp. 53–58. [\[CrossRef\]](#)
91. Thompson, D.R.; Di, J.; Daugherty, M.K. Teaching RFID information systems security. *IEEE Trans. Educ.* **2014**, *57*, 42–47. [\[CrossRef\]](#)
92. Tarn, J.M.; Chen, K. Mobile technology as a learning object and an exploration tool in an IS curriculum: An innovative instruction of wireless network security. *IEEE Trans. Educ.* **2006**, *49*, 193–198. [\[CrossRef\]](#)
93. Xiaohong, Y.; Percy, V.; Yaseen, Q.; Archer, R.; Huiming, Y.; Jinsheng, X. Visualization Tools for Teaching Computer Security. *ACM Trans. Comput. Educ. (TOCE)* **2010**, *9*, 1–28. [\[CrossRef\]](#)
94. Eliot, N.; Kendall, D.; Brockway, M. A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. *IEEE Access* **2018**, *6*, 34884–34895. [\[CrossRef\]](#)
95. Wannous, M.; Nakano, H. NVLab, a networking virtual web-based laboratory that implements virtualization and virtual network computing technologies. *IEEE Trans. Learn. Technol.* **2010**, *3*, 129–138. [\[CrossRef\]](#)
96. Luse, A.; Brown, A.; Rursch, J. Instruction in 802.11 Technology in Online Virtual Labs. *IEEE Trans. Educ.* **2021**, *64*, 12–17. [\[CrossRef\]](#)
97. Yu, H.; Liao, W.; Yuan, X.; Xu, J. Teaching a web security course to practice information assurance. In Proceedings of the 37th SIGCSE Technical Symposium on Computer Science Education, St. Louis, MO, USA, 23–27 February 2005; pp. 12–16. [\[CrossRef\]](#)
98. OConnor, T.; Stricklan, C. Teaching a Hands-On Mobile and Wireless Cybersecurity Course. In Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education, Virtual Event, 26 June–1 July 2021; pp. 296–302. [\[CrossRef\]](#)
99. Vekaria, K.B.; Calyam, P.; Wang, S.; Payyavula, R.; Rockey, M.; Ahmed, N. Cyber Range for Research-Inspired Learning of ‘Attack Defense by Pretense’ Principle and Practice. *IEEE Trans. Learn. Technol.* **2021**, *14*, 322–337. [\[CrossRef\]](#)
100. Radivojevic, Z.; Stanisavljevic, Z.; Punt, M. Configurable simulator for computer architecture and organization. *Comput. Appl. Eng. Educ.* **2018**, *26*, 1711–1724. [\[CrossRef\]](#)
101. Albert, W.B.; Tullis, T.S. *Measuring the User Experience: Collecting, Analyzing, and Presenting UX Metrics*; Morgan Kaufmann: Burlington, MA, USA, 2022; pp. 1–352. [\[CrossRef\]](#)
102. Ogrizović, M.; Vuletić, P.; Žarko Stanisavljević. Educational System for Demonstrating Remote Attacks on Android Devices. In *ICIST 2023: Disruptive Information Technologies for a Smart Society*; Springer: Cham, Switzerland, 2024; pp. 298–306. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.