Evaluating an Ethical Hacking Module: Case of a University in South Africa

Mpekoa Noluntu
University of Johannesburg, South Africa

noluntum@uj.ac.za

Abstract: The University of Johannesburg has Ethical Hacking content covered within the Information Security in the WWW module. This study was conducted at the University of Johannesburg, with honours students registered at the Academy of Computer Science and Software Engineering. This study aims to evaluate the Information Security in the WWW module. Specifically, it seeks to evaluate the content, teaching and learning, and extra activities such as participating in the first round of the National Cybersecurity Hackathon, through student perspectives. It also seeks to understand the views of the students on what they like the most about the learning module as a basis for continuous improvement. The instrument utilised was an amalgamation of module evaluation questionnaires in the body of knowledge. It was modified to suit the context of the study. The online questionnaire had both open-ended and closed questions that seek to get a better understanding of the concepts presented. The frequency distribution, percentage distribution, and weighted mean were calculated to offer the level of agreement and satisfaction. The findings suggest that students were satisfied with the content, teaching and learning, in the Information Security in the WWW module. The results further highlight some essential insights from the respondents that lecturers may consider when improving the instructional material. Further, considerations have been put forward for future improvement of the learning material.

Keywords: Module evaluation, Ethical hacking module, Student perspectives, Module improvement, Cybersecurity, cybersecurity hackathon

1. Introduction

The Fourth Industrial Revolution (4IR)'s technological convergence has increased connectivity, particularly through the Internet of Things (IoT) and smart devices. Systems that were previously isolated are now communicating with each other, sharing information, and establishing notifications (WEF, 2017; Ivanov & Das, 2020). A simple command like "Good Evening" to Amazon Alexa or Google Home can trigger a series of actions. This routine can automatically close your garage door, turn on your foyer, driveway, and living room lights, play specific music through a connected speaker, adjust the Climate Control thermostat to a comfortable setting, light the fireplace, and even start playing your favorite on-demand television show. While connected systems offer great convenience, they also pose a risk of cyberattacks. Any device connected to the Internet can be discovered and accessed by the public. This includes IoT sensors, smartphones, Wireless Fidelity (Wi-Fi) TVs, and even refrigerators, all openly communicating over your Wi-Fi network connected to the public Internet (Ivanov & Dolgui, 2021).

This digital revolution brings incredible conveniences. Users can access vast amounts of data, governments can address social challenges, and remote villages can connect with the rest of the country. Communities have transitioned into digital spaces, encompassing work, leisure, and commerce (WEF, 2017; Ivanov & Das, 2020). Digital tools in the classroom have given teachers and students increased opportunities. Teachers have been compelled to adapt their teaching strategies to support personalized learning, creativity, innovation, and problem-solving, and to allow more time for individual instruction (WTO, 2020). Many businesses suffered during and after the COVID-19 pandemic, with some Small to Medium Enterprises (SME)s closing down. 4IR has become more affordable and easier to implement, providing a viable recovery strategy for many businesses (Ivanov & Dolgui, 2021). Price Waterhouse Coopers (PwC) in 2018 conducted an annual global Chief Executive Officer (CEO) survey, where "81% of executives agreed that 4IR technologies created new efficiencies, and 78% agreed that they helped them automate tasks" (PwC, 2018). In the past systems were separated and now are connected and sharing data. According to Möller (2023), this connectedness also brings some drawbacks. When a device connects to the Internet, it becomes publicly accessible. As a result, these devices are vulnerable to cyberattacks (Singh & Kumar, 2020; Aphane, 2023).

Cybersecurity has become an essential part of everyday life due to the increasing frequency and severity of cyberattacks. The field of cybersecurity is highly challenging due to the rapid back-and-forth nature of the attack-defense dynamic (Cybersecurity Ventures, 2023). The national infrastructure, corporations, and agencies have been targeted by cyber-attacks, leading to the compromise of millions of sensitive data records, particularly in the financial and healthcare sectors (Singh & Kumar, 2020). These security breaches not only cause significant

financial losses but also severely damage the confidence of customers, business partners, and stakeholders (Möller, 2023; Kaspersky, 2023).

In the last quarter of 2022 and the first quarter of 2023, South Africa experienced a concerning 18.8% increase in cyberattacks. This highlights the growing threat of cybercrime and emphasizes the importance of individuals and organizations taking proactive measures to safeguard their digital assets (Kaspersky, 2023; DA, 2023). The 2022 Interpol report has labeled South Africa as the cybercrime hub of Africa, with hackers on the dark web showing interest in the country. A 2020 report by Accenture revealed that the country's internet users were less experienced and technically alert. Poor cybersecurity awareness and lack of end-user training have contributed to successful cyberattacks in South Africa (Möller, 2023; Ngoma, Keevy, & Rama, 2021).

Cybercrime poses a significant business risk in South Africa, with government departments expected to face a growing number of attacks. The economy suffers an estimated annual loss of 2.2 billion rands due to cybercrime (Kaspersky, 2023; Paganini, 2022; Mbelli & Dwolatzky, 2016). Cybersecurity involves technologies, processes, and practices to protect networks, devices, programs, and data from unauthorized access or damage (Cybersecurity Ventures, 2023; Ivanov & Das, 2020; Singh & Kumar, 2020).

Talents in cybersecurity are in high demand, leading to a surge in educational programs and pedagogical approaches in recent years (CyberSeek, 2024; Tredger, 2023). The paper is structured as follows: Section 2 gives a brief background on ethical hacking and the second part of the section provides a brief overview of the module. Section 3 provides a detailed research methodology for this study. Section 4 presents findings and discussion which include the course's strong points as well as potential areas for improvement. The conclusion is offered in Section 5.

2. Background

The concern regarding cybersecurity is rapidly growing in both public and private sectors. The increasing volume, velocity, and variety of data generated in cybersecurity analyses require well-equipped professionals to handle, analyze, and interpret these data (Zaman, Yi & Cheng, 2023; Ivanov & Das, 2020). In today's world, business professionals and public servants greatly need skills and knowledge in cybersecurity to combat the increasing cyber threats and issues. Creating suitable curricular materials and teaching methods could potentially help future cybersecurity professionals meet this demand (Wahsheh & Mekonnen, 2019; Al-Sherideh et al., 2023). According to the United States of America (U.S.) Bureau of Labor Statistics, the growth rate of jobs in information security is projected to be 37% from 2012 to 2022. At the same time, more than 209,000 cybersecurity jobs in the U.S. are unfilled every year. Cybersecurity education has been emphasized by several national organizations, which recognize securing cyberspace as critical (Nguyen, 2019; Faily, 2014; Bratus, Shubina & Locasto, 2010). The growing need for cybersecurity professionals in both the public and private sectors is a crucial task for higher education institutions. They must attract and educate the next generation of cybersecurity workforce and citizens who can contribute to national economic prosperity and security (Allison, 2023; Li et al., 2018; Levy, Ramim & Hackney, 2013). It is essential to prepare students for these challenges and improve cybersecurity education opportunities.

Ethical hacking involves identifying and correcting device flaws and vulnerabilities. It can be defined as a hacking mechanism without any harmful or destructive intent towards a network. Ethical hacking can also be described as a safety evaluation, training, or environment protection review for information technology (Sufatrio, and Chang, 2022; Yaacoub et al., 2021; Cangea, 2018). This method illustrates the risks encountered in an Information Technology (IT) environment and the measures to reduce those risks. The main goal of the ethical hacking service is to evaluate and provide a report to the owner on the security of the targeted systems and networks. Ethical hacking is conducted in conjunction with penetration testing techniques to assess security vulnerabilities (Wilson, 2022; Tabassum, Mohanan & Sharma, 2021; Messier, 2019). Various techniques are employed to obtain information, including information gathering, vulnerability scanning, exploitation, and test analysis (Luse & Shadbad, 2023). During training to become cybersecurity specialists, some of these concepts are discussed and expanded upon.

Module Background

Information Security in the WWW module at the University of Johannesburg (UJ), is a second-semester module from July–November. The module is taught over eleven (11) weeks and one (1) week for summative assessment. The contact (face-to-face) classes are in the evening for one hour and thirty minutes, once a week. The concepts covered are based on the internationally recognized Certified Ethical Hacker Study (CEH) Guide. The CEH study

guide is one of the distinguished course materials currently, as professionals with the CEH certification are well sought after both by private and public organizations.

The purpose of the module is to arm the students with fundamental knowledge and resources to shield an environment from known and potentially unknown dangers. In this module, students learn about the appropriate countermeasures that can and should be used to defend various online assets against threat actors. They also gain insight into the methods that these threat actors employ to subvert protection attempts. The goal is to protect not only the corporate environment but also the users interacting with the systems.

The following lectures (Table 1 below) were covered during the Information Security in the WWW module:

Table 1: Concepts covered in the Module

	Lecture Title	**Brief Objective of the Lecture**
Lecture 1	Introduction to Ethical Hacking	Background of ethical hacking and important terminology
Lecture 2	Footprinting & Scanning Networks	Introducing Footprinting and get understanding the information gathering methodology of hackers
Lecture 3	Enumeration & vulnerability analysis	Understand process of gaining complete access to the system by compromising the vulnerabilities identified in the first two phases
Lecture 4	Malware Threats	Understand types of malware threats and countermeasure techniques in preventing them
Lecture 5	System Hacking	Understanding privilege escalation techniques and techniques to create and maintain remote access to the system
Lecture 6	Sniffing	Discuss Active and passive sniffing, ARP poisoning and ethereal capture and display filters
Lecture 7	Reverse Engineering & SQL Injection	Understand the purpose of reverse engineering and the reverse Engineering Process. Understand the steps to conduct SQL injection and describe SQL injection countermeasures
Lecture 8	Social Engineering	Understand common types of social engineering attacks
Lecture 9	Cryptography	Give overview of Overview of cryptography and encryption techniques and describe public and private keys are generate
Lecture 10	Cheat Detection	Understanding Anti-Cheat, unethical means of winning and the impact of Cheating
National Hackathon	Cybersecurity hackathon	All students are to participate in the first-round of the National National Cybersecurity hackathon

Students who complete this course successfully should be able to: assess and measure threats to information assets; evaluate where information networks are most vulnerable, and critique security plans designed to protect information systems against attacks. Students should also be able to perform penetration tests into networks for evaluation purposes, develop an ongoing security strategy, and discuss the legal implications of ethical security circumvention.

3. Research Methodology

Through student perspectives, this study seeks to evaluate the Information Security in WWW module concepts. Specifically, it seeks to evaluate the content covered and extra activities such as participating in the first round of the National Cybersecurity Hackathon. To achieve the main aim of the study, the following sub-objectives were derived:

- Investigate and list concepts the participants understood.
- Investigate and list concepts the participants least understood.
- Identify areas of improvement

In this study, the researcher utilized a quantitative approach. In particular, the researcher employed a descriptive research design to analyze the participants' perceptions, opinions, or views on content and concepts covered in the Information Security in WWW module. The quantitative approach comprises studies that collect data using questionnaires to extrapolate findings from a sample to the entire population (Creswell & Creswell, 2017; Fowler, 2013). This study used the descriptive research design to answer the research questions in order to provide a clearer understanding of the concepts discussed in the Information Security in the WWW module. The

study was conducted at the University of Johannesburg and participants were registered students for the second semester of the 2024 academic year. The population under investigation are Information Security in the WWW honours module students. For the 2024 academic year, 47 students were registered for this module.

The selected data collection for this study is a survey, which is selected in accordance with the objectives of the problem under investigation (Tiala, 2022). The research instrument was designed using Google Forms. The research instrument was designed based on the result of reviewed related literature and studies and other sources. As a result, the instrument was an amalgamation of module evaluation questionnaires found in the body of knowledge (Rana et al., 2021; Connelly, 2014; Jones, 2012; Lewin, 2005). It was modified to suit the context of the study. The online questionnaire had both open-ended and closed questions that seek to get a better understanding of the concepts presented. The data collected was quantitative so therefore the data analysis was of a quantitative nature. The frequency distribution, percentage distribution, and weighted mean were calculated to offer the level of agreement and satisfaction.

4. Findings and Discussions

The instrument is composed of five sections (Section A – Section E). *Section A* is the invitation to participate in the survey and the consent form. *Section B* first gives the purpose of the module and then outlines the concepts covered in the module, and lastly assesses the concepts covered in the module. *Section C* uses a Likert-style rating to evaluate the concepts, then *Section D* allows participants to select concepts they most or least understood. *Section E* assesses the National hackathon cybersecurity activity.

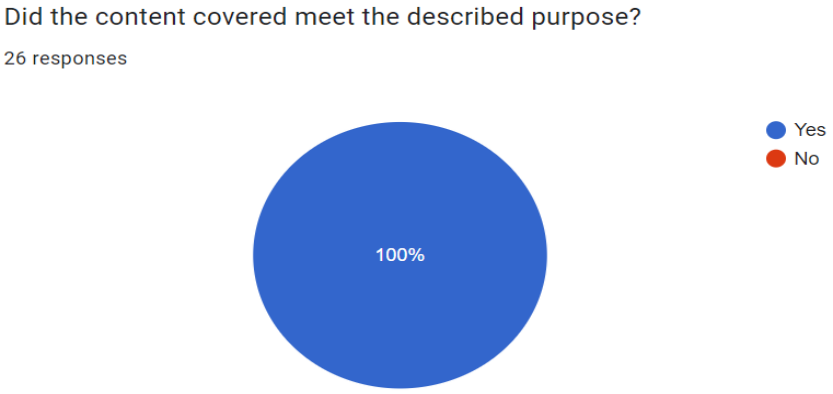

Figure 1: Participants' views on the described purpose

26 responses were received, out of 47 registered students (Figure 1 above). When the participants were asked if the content covered met the described purpose, all the participants agreed that the content met the described purpose. The findings section is sectioned based on the research sub-objectives.

4.1 Investigate and List Concepts the Participants Understood

The first sub-objective of this research was to investigate and list concepts the participants understood very well. As seen in Table 2 below, the participants used a Likert-style rating to evaluate each lecture, with 1 indicating least understood, 3 indicating understood, and 5 indicating very well understood.

Table 2: Concepts participants understood

	Lecture Title	1	3	5
Lecture 1	Introduction to Ethical Hacking	0%	23%	77%
Lecture 2	Footprinting & Scanning Networks	7%	15%	78%
Lecture 3	Enumeration & vulnerability analysis	0%	30%	70%
Lecture 4	Malware Threats	3%	3%	94%
Lecture 5	System Hacking	0%	19%	81%
Lecture 6	Sniffing	0%	23%	77%
Lecture 7	Reverse Engineering & SQL Injection	0%	23%	77%
Lecture 8	Social Engineering	0%	7%	93%

	Lecture Title	1	3	5
Lecture 9	Cryptography	0%	18%	82%
Lecture 10	Cheat Detection	0%	6%	94%
National Hackathon	Cybersecurity hackathon	0%	3%	97%

The rating for all the lectures ranged between 70% - 97%, meaning that students could understand and follow most of the concepts. The most popular lecture was the Cybersecurity hackathon where 97% of the participants indicated it was well understood, followed by the malware threat lecture with 94% of participants.

4.2 Investigate and List Concepts the Participants Least Understood

The second sub-objective of this research was to investigate and list concepts the participants least understood. Figure 2 below presents the responses from the participants when they were asked to indicate lectures they least understood.

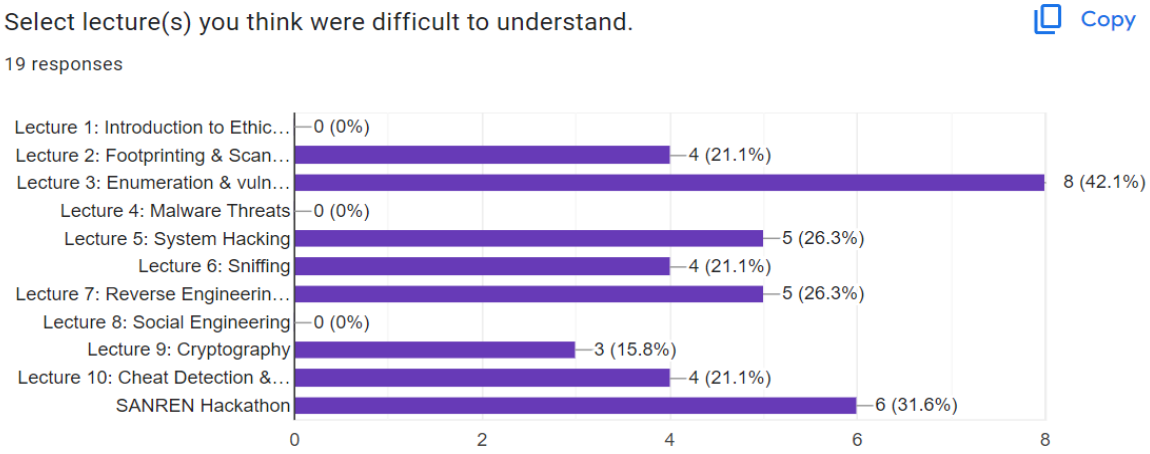

Figure 2: Concepts participants least understood

Some of the concepts that the participants indicated as least understood include the enumeration vulnerability analysis (42%), followed by 1st round of the Hackathon (32%), and then the system hacking and sniffing (26%) lecture. It is also noted that participants answered differently to both questions in Table 2 and Figure 2.

4.3 Identify Areas of Improvement

The final sub-objective of this research was to identify areas of improvement. The participants were asked if they enjoyed the module and 100% of the participants indicated they enjoyed the module (Figure 3) but 92% of the participants indicated that the time given for the module is not sufficient. Currently, the module is taught over a semester (6 months), which is eleven (11) weeks of contact (face-to-face) classes and one (1) week for summative assessment. The classes are in the evening for one hour and thirty minutes, once a week. Similar courses have been found to run for the same time or even shorter such as Demetrio, Lagorio, Ribaudo, Russo, Valenza (2019) and Andreatos (2023).

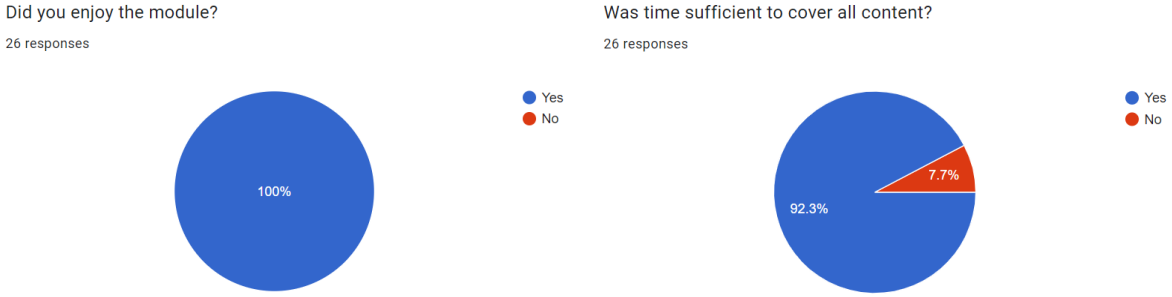

Figure 3: Participants' views on overall module

The participants were asked what changes they would recommend to make the module more effective, the following answers were received (Figure 4).

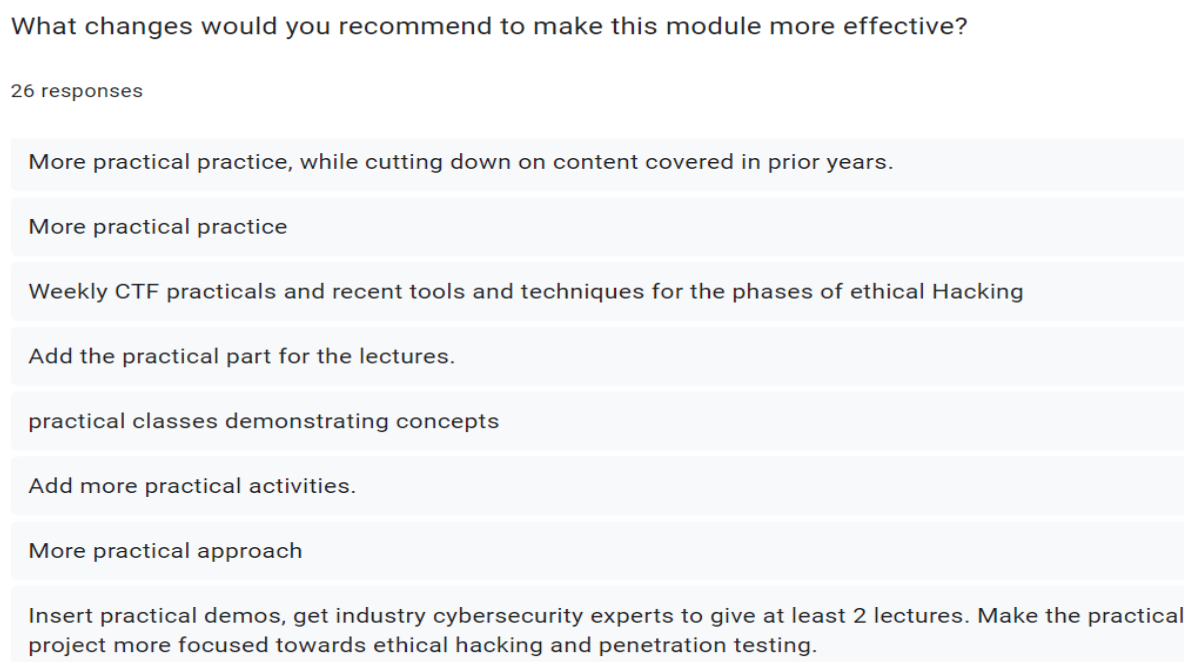

Figure 4: Participants' recommendations

The majority of participants have requested that the module be made more practical, with increased opportunities to exercise their theoretical knowledge. However, due to time constraints, there is limited time for practical work. One proposed solution is to explore similar modules that have successfully implemented practical components, such as Demetrio, Lagorio, Ribaudo, Russo, Valenza (2019) and Andreatos (2023). The study observed that although most of the students did not have any prior knowledge or experience on cybersecurity and ethical hacking, the participants responded positively, indicating that they understood most of the concepts with very few participants who did not understand some concepts. This is similar to other studies such as Yaacoub et al. (2021), where participants were exposed to capture-the-flag exercises and ethical hacking principles.

5. Conclusion

The field of cybersecurity is currently experiencing a high demand for talented individuals, leading to a significant increase in educational programs and innovative teaching methods in recent years. These programs provide training for cyberwarriors on how to assess and measure threats to information assets, evaluate the most vulnerable points in information networks, and critique security plans designed to protect information systems against attacks. This research evaluated the Information Security in WWW module concepts presented to honours students at a university in SA. It aims to assess the covered content and additional activities, such as participating in the initial round of the National Cybersecurity Hackathon. The results indicate that all participants had a good understanding of the covered content. The most popular lecture was the Cybersecurity hackathon, which the participants found well understood, followed by the lecture on malware threats. Some of the concepts indicated as least understood by the participants include enumeration vulnerability analysis, the first round of the Hackathon, and the system hacking and sniffing lecture. There was a conflict in ideas as depicted above, with some participants understanding the hackathon and others not comprehending it. Most of the participants indicated that they enjoyed the module and agreed that the content met the purpose described. Some of the changes recommended include increasing the time for the module, and that the module be made more practical, with increased opportunities for hands-on exercises to better understand the theory. The number of participants were a limitation to this study, as it restricts the researcher from generalizing the findings. This study is ongoing, the findings from each of the surveys could be compared and further conclusions could be drawn from there. Additionally, subsequent surveys will collect demographic data, where this can be part of the findings. This study can also be improved by utilizing a mixed methods research that combines both qualitative and quantitative data for data triangulation to offer more validity and reliability.

References

Allison, J. (2023). Devising a cyber security management module through integrated course design. Journal of Further and Higher Education, 47(10), 1389-1403.

Al-Sherideh, A. S., Maabreh, K., Maabreh, M., Al Mousa, M. R., and Asassfeh, M. (2023). Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study. International Journal of Advanced Computer Science and Applications, 14(5).

Andreatos, A. (2023). An educational scenario for teaching cyber security using low-cost equipment and open source software. *Proceedings of the ECCWS* pp 44- 53.

Aphane, M. P. (2023). Cybersecurity Awareness on Cybercrime Among the Youth in Gauteng Province. International Journal of Social Science Research and Review, 6(8), 23-32.

Bratus, S., Shubina, A., and Locasto, M. E. (2010). Teaching the principles of the hacker curriculum to undergraduates. In Proceedings of the 41st ACM technical symposium on computer science education (pp. 122-126).

Cangea, O. (2018). Ethical Hacking Solution to Defeat Cyber Attacks. Petroleum-Gas University of Ploiesti Bulletin, Technical Series, 70(2).

Connelly, L. M. (2014). Ethical considerations in research studies. Medsurg nursing, 23(1), 54-56.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Cybersecurity Ventures (2023). Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

CyberSeek (2024). Cybersecurity talent gaps. https://www.cyberseek.org/heatmap.html

Demetrio, L., Lagorio, G., Ribaudo, M., Russo, E. and Valenza, A. (2019). ZenHackAdemy: Ethical Hacking@ DIBRIS. In CSEDU (1) (pp. 405-413).

Faily, S. (2014). Ethical hacking assessment as a vehicle for undergraduate cyber-security education. In Uhomoibhi, J.O., Linecar, P., Barikzai, S., Ross, M. and Staples, G. (eds.) Global issues in IT education: proceedings of the 19th International conference on software process improvement research, education and training (INSPIRE 2014), Southampton, UK. Southampton: Solent University, pages 79-90.

Fowler Jr, F. J. (2013). Survey research methods. Sage publications.

Ivanov, D. and Das, A. (2020). 'Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: A research note', International Journal of Integrated Supply Management 13(1), 90–102. https://doi.org/10.1504/IJISM.2020.107780

Ivanov, D. and Dolgui, A. (2021). 'A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0', Production Planning & Control 32(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

Jones, K. (2012). A regrettable oversight or a significant omission?: Ethical considerations in quantitative research in education. In Situated ethics in educational research (pp. 147-161). Routledge.

Levy, Y., Ramim, M. M., and Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. Journal of Computer Information Systems, 53(3), 75-84.

Lewin, C. (2005). Elementary quantitative methods. Research methods in the social sciences, 215-225.

Li, L., Li, Z., Shahriar, H., Rutherfoord, R. H., Peltsverger, S., and Tatum, D. (2018). Ethical Hacking for Effective Defense.

Luse, A., and Shadbad, F. N. (2023). Teaching Tip: Hackalytics: Using Computer Hacking to Engage Students in Analytics. Journal of Information Systems Education, 34(4), 370-386.

Mbelli, T. M., and Dwolatzky, B. (2016). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 1-6). IEEE.

Messier, R. (2019). CEH v10 Certified Ethical Hacker Study Guide. John Wiley & Sons.

Möller, D. P. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 231-271). Cham: Springer Nature Switzerland.

Nguyen, T. N. (2019). Certified ethical hacker v. 10 online course: a case study. In Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning (pp. 168-173).

PwC (2018). Navigating the rising tide of uncertainty, 23rd Annual Global CEO Survey. Accessed 09 November 2023 at https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2020.html

Rana, J., Gutierrez, P. L., & Oldroyd, J. C. (2021). Quantitative Methods. Global Encyclopedia of Public Administration, Public Policy, and Governance, 1-6.

Singh, S., and Kumar, S. (2020). The times of cyber attacks. Acta Technica Corviniensis-Bulletin of Engineering, 13(3), 133-137.

Sufatrio, Vykopal, J., and Chang, E. C. (2022). Collaborative Paradigm of Teaching Penetration Testing using Real-World University Applications. In Proceedings of the 24th Australasian Computing Education Conference (pp. 114-122).

Tabassum, M., Mohanan, S., and Sharma, T. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. Nternational Journal of Innovation in Computational Science and Engineering, 2(4), 9-22.

Tiala, S. (2022). Beginning the Investigation: The Research Question. In Conducting Undergraduate Research in Education (pp. 21-37). Routledge.

Tredger C. (2023). South Africa under pressure to fill cyber security skills gap. https://www.itweb.co.za/article/south-africa-under-pressure-to-fill-cyber-security-skills-gap/DZQ587V8bjrqzXy2

Wahsheh, L. A., and Mekonnen, B. (2019). Practical cyber security training exercises. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 48-53). IEEE.

Wilson, R. (2022). Hands-on ethical hacking and network defense. Cengage Learning.

World Economic Forum (WEF). (2017). Impact of the Fourth Industrial Revolution on supply chains, System Initiative on Shaping the Future of Production, World Economic Forum, Geneva.

World Trade Organisation (WTO). (2020). E-commerce, trade and the Covid-19 pandemic, pp. 1–8, WTO Secretariat, Geneva.

Yaacoub, J. P. A., Noura, H. N., Salman, O., and Chehab, A. (2021). A survey on ethical hacking: issues and challenges. arXiv preprint arXiv:2103.15072.

Zaman, T., Yi, A. L. H., and Cheng, H. Y. (2023). Scaffolding Undergraduate Students' Ethical Cyber Behaviour With Philosophy and Theory. In Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 112-129). IGI Global.