Annotated Bibliography – 1:

Bowen. (2017). The Limits of Hacking Composition Pedagogy. Computers and Composition, 43, 1–14. https://doi.org/10.1016/j.compcom.2016.11.001

The essay synthesises a survey in the field of literature on hacking and its contemporary practices in opened ended competitions called hackathons. With so many arising opportunities, the author takes a survey over to understand the people and the caution it could provoke if Hacking is adopted as a form of education and ultimately to present a more sensible vocabulary or a composition for hacking. This source, which was published over five years back, was ahead of its time to convince such a topic of a more stereotypical audience. There are terminologies which can't be interchanged. Still, there are terms in the enormous scope of computer science, especially in hacking which could change the intention of the basic idea to be presented. Therefore, the author has discussed the significance of the terms used in the Hacking pedagogy.

Hacking has become more of a taboo in the open society, and illegal or mishandling computer technology has gone way out of hand. But there are terms that the general audience or even a couple of cyber experts (Hackathon participants) use with regard to something else that could change the perspective and the idea perceived by the audience. Taking it away from this for an example: A person does not have to be exceptional in mathematics to code his way out – instead, mathematics develops the logical reasoning behind his solutions to think from various perspectives. Therefore, the survey performed in this article states has emphasised the significance of the terminologies being used.

Annotated Bibliography – 2:

Childers, N. *et al.* (2010). Organizing Large Scale Hacking Competitions. In: Kreibich, C., Jahnke, M. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2010. Lecture Notes in Computer Science, vol 6201. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14215-4_8

Apart from hackathons, the author has reviewed the process of conducting large-scale hacking and security competitions and has discussed the problems that have to arise in them to set a framework or a guideline to how matches should be performed to make it fair among other students. The source does not cover the financials or expenses of the competitors, which play a considerable role when running a competition on such a large scale. These competitions represent and simulate the real world; therefore, an enormous amount of power and technology will be used; thus, costing is an important aspect it lacks. The intended audience is other competition conductors and young enthusiasts who would are interested in the backend of a huge competition.

Since every other source talks about Hackathons – this article gives us insight into the other perspective of hacking competitions on how these are conducted and the struggle they go through to make this possible. These competitions have different characteristics, configurations and goals every year to live security exercises involving dozens of universities worldwide. There are two other competitions *(Treasure Hunt and a Bot-net-inspired competition)* which serves as the most extensive security exercises ever attempted, where hundreds of people have come to take part in these competitions. From the past competitions they've conducted – they've come up

with a structured guideline to make the competitions fair for the other educators who want to pursue similar and for the student.

Annotated Bibliography – 3:

Hartley. (2015). Ethical hacking pedagogy: An analysis and overview of teaching students to hack. Journal of International Technology and Information Management, 24(4), 95–.

This article provides distinct research conducted, underlining the analysis of an ethical pedagogical to facilitate future information security professionals. The source covers the significant aspects of what's required for the written assignment. Moreover, it covers a lot more background context to give a focused perspective on what the author is saying. The author is trying to persuade the audience by justifying how Ethical hacking as a course is significant considering the upcoming crimes circulating the cyberspace and feels like we're not well equipped for it since we're only learning to defend ourselves but not to attack – therefore, providing the offence side of it will make it more secure. The article's main argument is to provide research to see if it's a course with potential as it sounds theoretical.

Future information security professionals are adapted to have the same skill as attackers to recognise and defend networks from intrusion adequately. But when this comes to a profession – people tend to lean towards the safer side of the spectrum to get a safe and secure job. On the contrary, numerous institutions educate students on the fundamentals of Cybersecurity and how to protect themselves from an attacker but never really teach them the offensive side. When the students get exposed to what the attackers are getting exposed to, this

can stop even more cyber crimes. Still moreover, this article discusses if this adaptive process would be a viable option through research and concludes with its findings.

Annotated Bibliography – 4:

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. In *Proceedings of the EDSIG Conference ISSN* (Vol. 2473, p. 3857). http://proc.iscap.info/2017/pdf/4341.pdf

The author has understood the technological advancement around him and has researched a wider spectrum of ethical hacking and cybersecurity, covering the information security trends and methods over the pedagogical approach and finally examining the best practices in the field. The author has used several hacking incidents as an example not just to support his claim but also to connect it back to the techniques the hackers have exploited. The author has also made an interesting argument of making the hackers and the cybersecurity specialists to make them work together for a more competitive battleground for both sides.

Hands-on approach, soft skills and contributed lab sessions are proven ways to enhance new techniques to protect ourselves from hackers. Since this type of educational system covers both the offence and the defensive side of the barriers, this gives more opportunity for the students and for the service providers like businesses and governments to be even more cautious. Also, depending upon the trends of attacks that are being made – they not only monitor the student but also adapt the students to what's going on around them. Thus concluding the significance of cybersecurity professionals and emphasizing on the necessity of training hackers and cybersecurity experts for a more technical expertise.

Annotated Bibliography – 5:

Kessel. (2019). Pracademic collaboration: Hacking into the future of legal education. Alternative Law Journal, 44(1), 73–75. https://doi.org/10.1177/1037969X18814980

The author does not necessarily have a background connected to it but has developed a modern solution for a current problem. He introduces a term called "pracademic", – which is a teaching style born out of concern since the professional programs developed are misaligned with the natural market's needs. The source covers so many ifs and is only being taken from a positive point of view. The author has connected creative knowledge applications with hackathons, providing us more insight into practical-academic. The author's argument is to expose graduate students to a broader range of interdisciplinary viewpoints – may be the key to nurturing creative and digital capabilities. He thinks creative hacking and multidisciplinary collaboration will allow the participants to draw their resources – to provide innovative solutions that can significantly impact the profession.

Looking at the article's bacground, there're way too many grey spaces in it, which makes this whole concept of "practice-based learning" a joke. Annotated Journal – 2 has discussed the ethical concerns, and all of the research sources point out producing better results when working collaboratively – even though this article agrees with it to a certain extent, it's making individuals come up with innovative solutions which not only contradicts with other significant sources – but multiple kinds of researches have proved that collaborative work can be more effective and efficient. Similar to the second and third journals, this article has also been connected to hackathons to support its idea. But the pracademic aspect made sense since the people in the field are misaligned and have to get back on track.

Annotated Bibliography – 6:

Trabelsi, & McCoey, M. (2016). Ethical Hacking in Information Security Curricula. International Journal of Information and Communication Technology Education, 12(1), 1–10. https://doi.org/10.4018/IJICTE.2016010101

The author has proposed how Ethical Hacking in Cyber Security is crucial to the Information Security curriculum. He has discussed how the defensive strategies extended to the offensive security component are necessary to make the professionals even stronger. He has addressed the learning outcomes through what he can achieve through lab exercises. The curriculum would have ethical implications associated with introducing these labs. The discussions are based upon the results produced by the students in the labs but, most importantly, the student behaviour after acquiring these skills. He has also researched the approaches and the outcomes that could be produced by teaching these offensive techniques to the students.

With a vision of providing a powerful insight which could affect the way the world works, the article covers the opportunities, threats, pros and cons of bringing up such an educational system and how they could be tackled. Moreover, he has discussed how this could be the future of cybersecurity. This is more like teaching a child to use a sword, and the chances it could fall into the wrong hands are much longer. The survey evaluating individuals was not a very efficient way of qualifying.