Review on Teaching Ethical Hacking

Sushil Bhardwaj

Assistant Professor, Department of Computer Applications, RIMT University, Mandi Gobindgarh, Punjab, India

Correspondence should be addressed to Sushil Bhardwaj; sushilbhardwaj@rimt.ac.in

ABSTRACT- The word hacker generally characterize the practice or performance of investigating & carry out trial with computer networks as computer communications grew more ubiquitous with the emergence of the Internet. However, when devices with tools and connected network became more commercialized, the system also became assets with ostensible limitations, & violating such borders became illegal. The number of programs teaching ethical hacking is rapidly increasing. The requirement for a comprehensive understanding of tactics and assailants is at the heart of the case for training in ethical hacking field. Many peoples argue, however, that getting training in offensive hacking skills advances communal menace by promising followers to take part in illegitimate behaviour. Ethics instruction pervades associated curricula, according to proponents of teaching ethical hacking, giving students enough preparation to recognize the hazards and adopt healthy actions. This article looks at ways to reduce the danger of students using abilities learned in an ethical hacking course to perform illegal activities outside of the classroom.

KEYWORDS- Ethical Hacking, Hacking, Hacking Education, Hacking Ethics, White Hat Hacking.

I. INTRODUCTION

Hacking arose from a long tradition of software developers cooperating to produce novel, aesthetically pleasing, and technically virtuosic software products [1][2]. The word hacker essentially characterize practice of investigating and try out with interconnected devices as computer communications grew more ubiquitous with the emergence of the Internet. However, when utilities and connected gadgets became more commercialized, they apparently turn into assets with ostensible limitations, & violating such borders became illegal. The phrases white, grey and black hat hacker shall primarily be used throughout this article. A hacker who usually is referred to as white-hat is someone who is devoted to abiding by all legitimate and supervisory legislation as well as stated ethical standards that are relevant to the activity at hand [3–6]. A black-hat hacker, on the other hand, is a hacker who either disregards or deliberately disregards legal or regulatory legislation, presumably with little regard for ethical standards.

As students attempt to complete course requirements, open usage of software and networks is frequently encouraged, if not compulsory, in academic programs. Pupils are then forced to collaborate with several other learners on joint ventures in very same way that premature hacking persons did [7]. Occasionally, though, allocation of programme or device is prohibited. Learners are usually told in case assets may be commonly used and if they can't, and there's minimal pressure on them to decide if it's okay to commonly use or access other people's data or systems. It's uncertain if academic training environments offer students with a safe atmosphere in which to practice ethical behaviour [8–13]. This article is the result of a debate about whether students are receiving adequate cares & familiarities to assist in making ethical judgments when using security related drills. Kicking out or persuasions for hacking goings-on among students are rising fastly, indicating that more has to be done to safeguard pupils.

Over the last decade, ethical hacking courses have grown in popularity, with an increasing number of colleges participating [14]. The curriculum for such courses usually includes ethics and law instruction, as well as a demand for academics to demonstrate acceptable behaviour when it comes to ethical hacking. Learners who gains knowledge historically unlawful computing abilities in the process of swotting hardware safekeeping will utilize such talents for superior good considerably frequently than they would use the same illicitly or dishonestly, according to the risks associated with teaching such classes [15–19]. When it comes to safeguarding society from students' criminal acts, this explanation may suffice; nonetheless, it is crucial to highlight that teaching hacking poses two distinct hazards. Apart from the jeopardy to learners in the program who might usually be enticed into criminal behaviour by the knowledge gained, there is always a chance of risk to humanity if someone performs ill use of the facilities they were imparted.

Guarding the initial learners is especially essential as they are not aware of their hacking related deeds [20]. If we consider few of the recent research, both kinds of hackers i.e., white or black are cognisant of the repercussions of unauthorised hacking, while a group of college going learners are unacquainted. “Hackers are well aware that if they are found engaged in illicit hacking operations, their lives would be severely disrupted,” according to the research. This demonstrates the US government's success in informing the hacker community about the danger of engaging in unlawful hacking operations. Meanwhile, the message is not getting across to the college student population. There's also the question of whether students get the hands-on experience which is required to learn proper ethics or not.

II. METHODOLOGY

Apart from available knowledge of ethical hacking (EH), which has been in existence for almost few decades, a lookout of the topic showed very little assistance in training learners to properly employ basic hacking related abilities gained at university level. As Subject Matter Experts (SMEs), three senior information security experts were inquired what sort of learning or combination of training would help university learners comprehend & apply EH instruction. Every discussed SMEs has a Chief Information Security Officer, who employ & evaluate information security specialists on a regular basis. Because of not enough material on which to base particular questions, the SMEs suggested gathering information from a larger group of experts and rejecting the notion of a specific questionnaire for interviews. Instead, they advocated for information security experts to be permitted to reply without prompting with what they feel will help college students interested in employment in the field avoid unlawful acts. Furthermore, the SMEs suggested pursuing just the "low hanging fruit," which was defined as things recommended by at least 25% of respondents.

All of the interviewers claimed to be information security experts with at least a year of experience. In the spring of 2013, 205 meetings have been performed at several security conferences in the Southwest USA. One event was accessible to all information security experts, one was aimed at CISOs and mandated an invitation and credentials to attend, and one was specific to the motion picture business and required an invite along with respective authorisations to attend the same. From the three events, there were 121, 29, and 36 responders, correspondingly.

Despite the fact that < 16% of participating peoples identified as hacking professionals, they were all employed in some information security business on some great positions. Many of them has dealt with hacking in various roles in the information security area, including policy creation, training, auditing, managing, and practicing.

Respondents were requested to provide their names, firm affiliations, job titles, and tenure of skill familiarity in the field of data privacy. They were also probed if EH should be taught or not as curriculum of colleges, and if they had any suggestions for helping students follow the ethical principles provided in the certified ethical hacking literature.

A. Data Collection:

In case participating peoples matched with the study's requirements, they were queried to suggest undertakings that might aid them better apprehend & follow moral norms. When comparable replies were grouped together, they were merged into categories that were established after the data was gathered. After suggestion of the SMEs, every commendation grouping that received more than 23% approval from participating peoples was considered & subsequently investigated using hypothetical writings.

Each of the 202 contenders agreed that EH should be taught in university curriculum, and the majority of them gave one or more ideas for safeguarding pupils. The proposals were divided into four categories, with four of them meeting the inclusion criteria of 25%. Eighty percent (39 percent) or more of the respondents approved each of these four categories:

- Competition
- Recognition
- Social interaction or support system
- Ongoing skills development

All of the above categories was researched in order to come up with particular recommendations, which are presented in this article. Three extra categories were formed since the 25 percent inclusion criteria were not met:

- Cybersecurity internships
- Interaction with cybersecurity-related law enforcement

III. DISCUSSION

A. Social Interaction:

Positive social groups were cited more frequently by study participants than any of the other recommendations [21]. On all cybersecurity sector, group affiliation & collaboration are obvious, and the value of these affiliations is clear. If we focus towards white-hat hacking, there are several CERTs (Computer's Extra Response Teams), the CSGE (Cyber Safety Group of Europe), and numerous more. Black-hat culprits are to be expected to keep a little outline, but the commonly available group peoples are aware of, show that mutual support is important to felonious hacking professionals as well. A Bing searching report for "cyber security groups" returned almost 6,555 results, indicating that there is a huge number organizations of that type. Such connections are in the offing to be a beneficial method for any sort of hacking professionals to share technical information and develop abilities, but their significance certainly extends beyond that.

White-hat hackers that support the law create societies of practice to assist in the development of EH agendas to govern actions inside field of study. Peer groups and networks of social support are always guiding technological improvement as well as acquire how to cope with challenging legitimate & supervisory challenges in legal and ethical ways that are consistent with the groups EH agendas. Black-hat hacking professionals that feel their cause is more important than the law establish like-mindedness groups with other peoples who ethically justify group's divergent activity.

White-hat and black-hat hacking professionals are both worried about recognition of their respective conduct within their class, as per the studied works of several authors. A way to proceed is much probable to be adopted provided the same is deemed morally permissible by own colleagues. Becoming a part of a professional community, including the social identity hypothesis,, leads a participant to develop choices to fall halfway within their unique individual opinions and those that the team considers appropriate. Importantly, the self-consciousness argument entails that organizational users should categorize options as either conforming to group consensus or not. As a consequence, an individual is influenced not just by the social circle, and yet individuals were generally likely to accept the team's delineations, including such legal versus unlawful behaviors. As a consequence, if the society doesn't quite tolerate a predefined action, people are highly likely to shun it.

- Proposition 1: Creating student peer networks that promote white-hat hacking methods while adhering to ethical and moral norms based on the rule of law would minimize the chance of students engaging in unethical behaviour.

B. Competition:

It is to have carved out a substantial place for the selves in the world of EH tutoring [22][23]. There are several essays published in favour of the learning breakthroughs and benefits made available by cybersecurity contests. The usefulness of cybersecurity competition in developing student abilities was backed up by comments from respondents in this study. This article, on the other hand, focuses solely on the effect of cybersecurity contests in lowering possible criminal conduct among ethical hacking students.

While a study of the literature found no direct evidence that contests encourage obedience to moral norms, having a number of unplanned affirmative effects. The fact that a number of learners get the 1st genuine and prominent working benefits. The contests themselves, as well as accompanying job fairs and industry engagement, elicit enthusiasm for the chances that lie in advance, several of them shall be lost if a felonious persuasion were to occur. Countless contests also include "real-world" set-ups that compel competitors to think about the moral and permissible ramifications of the acts. Students may be expected to show moral concerns or challenges before a group of professional and technical peoples in certain circumstances, which gives essential practice using ethical hacking instruction. Following this kind of occurrence, feedback could assist learners realize where their desire to accomplish given work effectively in an antagonism might have driven the learners to breach an ethics.

Furthermore, cyber security contests countenance the learners to engage with each other as well as trade experts, broadening the opportunities accessible. Being a learner allows them to become more aware of the breadth of the civic available to white-hat hacking professionals, the power of dealing with community peoples will have an even bigger impact on their conduct. Lastly, contests have a strong impact that mainly assist learners enhanced grasp the two distinct cybersecurity groupings they are allowed to pick from. White-hat hacking competitions provide a fantastic chance for students to learn about the differences between the white-hat and black-hat sides of the cybersecurity business, with a focus on the advantages of white-hat hacking and the risks of black-hat.

C. Recognition:

The desire for hackers to be recognized for their skills and achievements was acknowledged by industry respondents as being extremely essential for many in the hacking community. Hackers join a community for a variety of reasons, including mutual support and the desire to be recognized within it. The hacker community has a strong need for fame, and the difficulty to achieve notoriety through white-hat hacking activities may push students toward black-hat hacking. Recognition might come from winning a competition, but it can also come from observing and tracking student actions on learning materials and in the classroom, in addition to contests and other outside activities.

Leader-boards, sometimes known as scoreboards, have long been used in sporting arenas to track competitors' performance. The National Cyber League (NCL) and other cybersecurity contests already employ this method. Similar leader-boards in academic programs can help students comprehend how their abilities compare to those of their peers and recognize outstanding performers.

- Proposition 3: Recognizing white-hat hacking efforts that are relevant to a student's peer group reduces the chance that a student will need to participate in black-hat activities in order to achieve attention and reinforces the importance of white-hat activities.

D. Ongoing Skills Development:

Hackers must continue to enhance their abilities on a regular basis. A hacker is a provider of inventive and elegant solutions, which implies that sustaining one's hacker identity necessitates a never-ending dedication to taking on and conquering ever-increasing obstacles[24][25]. Hackers reach a state of flow, which is a phrase used in the communications literature to describe how activities flow from one to the next easily and almost effortlessly. Flow is an internal motivator that occurs when a participant encounters problems that are at the cutting edge of his or her skill level and effectively overcomes them. Participants in video games are a good example, since they will play for hours, confronting challenge after challenge, with no reward other than the internal satisfaction associated with the work and possibly some bragging rights within the participant's social circle.

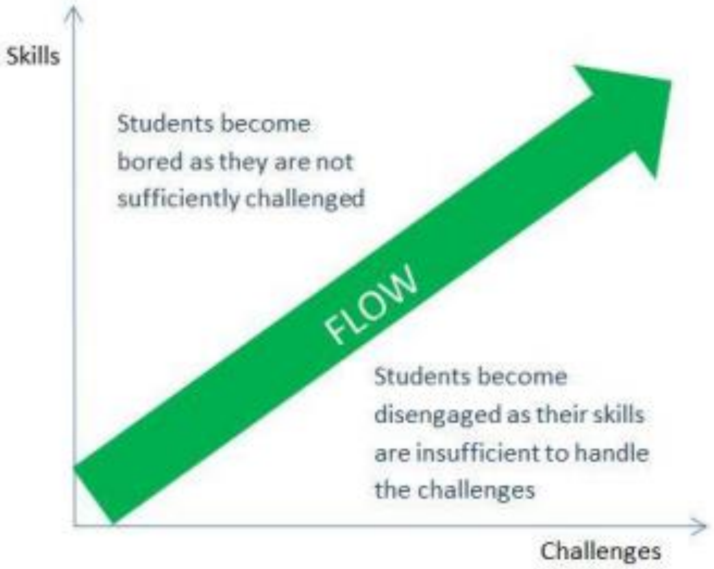
Skills
Students become bored as they are not sufficiently challenged
FLOW
Students become disengaged as their skills are insufficient to handle the challenges
Challenges

Fig. 1: Relationship of Skills vs Challenges.

For academic programs, this means that they must be prepared to raise the obstacles they face in order to reach and maintain their students' skill levels. The continuum of challenges necessary to guarantee students receive adequate basic tasks at the beginning of the learning process and a sufficient tough activity as their skill development process matures is depicted in Fig. 1. Academic partnerships, as well as ties with government and business, may be critical components in sustaining an appropriate degree of difficulty for students. Learning initiatives, research projects, contests, internships, and other forms of collaboration might be included.

- Proposition 4: Providing tasks that are appropriately suited to students' ability levels would minimize the chance of pupils engaging in black-hat behaviour. Students who do not reach a state of flow because their abilities are insufficient to properly handle the obstacles they are encountering may benefit from sufficiently basic activities.

E. Limitations:

It's worth noting that questioning security experts at conferences may have impacted the results because issues like mutual support and competitiveness were discussed. However, this author believes that this impact is not an issue because the presentations were not affected by the study and are merely another evidence of how important these topics are in the cybersecurity industry.

IV. CONCLUSION

It is apparent that cyber security schools ought to address the role that EH shall play in their curricula, given the universal support of 206 industry professionals. Notwithstanding, it is vitally important to consider specific risks that learners confront & strategies to manage the same. Considering overall catastrophic potential of the skills getting imparted and the allure of negative influencing factors on students, promoting EH is a serious task. This is particularly significant when the privacy & safety concerns kids face throughout completing their university qualifications are complex, and it may be difficult to understand how to implement the hacking training ethically they've acquired in classroom. Professors possess an ethical commitment to do all necessary to ensure that learners get prepared to face the difficulties with the capabilities we provide.

Teaching students the significance of professional networks and getting them involved with a supportive peer group is essential, according to both interviews with industry professionals and a review of the research. Recommendations for the formation of student peer networks that provide support, as well as, ideally, connections with business associations and appropriate law enforcement authorities, are an essential next step in the endeavour to safeguard students in ethical hacking courses. The importance of current best practice in teaching ethical hacking (teaching ethics, alerting pupils of criminal consequences, and modelling ethical actions) cannot be overstated. However, well-designed social interactions and support, competitiveness, recognition, and adequate obstacles can assist students avoid criminal conduct while simultaneously improving cybersecurity programs.

REFERENCES

1. Is Ethical Hacking Ethical? Int J Eng Sci Technol. 2011;
2. Hartley R, Medlin D, Houlik Z. Ethical Hacking: Educating Future Cybersecurity Professionals. Proc EDSIG Conf. 2017;
3. Ghai W, Kumar S, Athavale VA. Using gaussian mixtures on triphone acoustic modelling-based punjabi continuous speech recognition. In: Advances in Intelligent Systems and Computing. 2021.
4. Khatri M, Kumar A. Stability Inspection of Isolated Hydro Power Plant with Cuttlefish Algorithm. In: 2020 International Conference on Decision Aid Sciences and Application, DASA 2020. 2020.
5. Sharma K, Goswami L. RFID based Smart Railway

Pantograph Control in a Different Phase of Power Line. In: Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020. 2020.

6. Goswami L, Kaushik MK, Sikka R, Anand V, Prasad Sharma K, Singh Solanki M. IOT Based Fault Detection of Underground Cables through Node MCU Module. In: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020. 2020.

7. Munjal MN. Ethical Hacking: an Impact on Society. Cyber Times Int J Technol Manag. 2013;

8. Solanki MS, Sharma DKP, Goswami L, Sikka R, Anand V. Automatic Identification of Temples in Digital Images through Scale Invariant Feature Transform. In: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020. 2020.

9. Kumar A, Jain A. Image smog restoration using oblique gradient profile prior and energy minimization. Front Comput Sci. 2021;

10. Gupta N, Vaisla KS, Jain A, Kumar A, Kumar R. Performance Analysis of AODV Routing for Wireless Sensor Network in FPGA Hardware. Comput Syst Sci Eng. 2021;

11. Gupta N, Jain A, Vaisla KS, Kumar A, Kumar R. Performance analysis of DSDV and OLSR wireless sensor network routing protocols using FPGA hardware and machine learning. Multimed Tools Appl. 2021;

12. Gupta B, Gola KK, Dhingra M. HEPSO: an efficient sensor node redeployment strategy based on hybrid optimization algorithm in UWASN. Wirel Networks. 2021;

13. Kumar Gola K, Chaurasia N, Gupta B, Singh Niranjan D. Sea lion optimization algorithm based node deployment strategy in underwater acoustic sensor network. Int J Commun Syst. 2021;

14. Trabelsi Z, McCoey M. Ethical hacking in information security curricula. Int J Inf Commun Technol Educ. 2016;

15. Khanna R, Verma S, Biswas R, Singh JB. Implementation of branch delay in Superscalar processors by reducing branch penalties. In: 2010 IEEE 2nd International Advance Computing Conference, IACC 2010. 2010.

16. Gupta H, Kumar S, Yadav D, Verma OP, Sharma TK, Ahn CW, et al. Data analytics and mathematical modeling for simulating the dynamics of COVID-19 epidemic—a case study of India. Electron. 2021;

17. Gupta H, Varshney H, Sharma TK, Pachauri N, Verma OP. Comparative performance analysis of quantum machine learning with deep learning for diabetes prediction. Complex Intell Syst. 2021;

18. Sharma TK. Enhanced butterfly optimization algorithm for reliability optimization problems. J Ambient Intell Humaniz Comput. 2021;

19. Hirawat A, Taterh S, Sharma TK. A dynamic window-size based segmentation technique to detect driver entry and exit from a car. J King Saud Univ - Comput Inf Sci. 2021;

20. Hernández M, Baquero L, Gil C. Ethical Hacking on Mobile Devices: Considerations and practical uses. Int J Appl Eng Res. 2018;

21. Sahare B, Naik A, Khandey S. Study Of Ethical Hacking. Int J Comput Sci Trends Technol. 2014;

22. Dark M. Advancing cybersecurity education. IEEE Secur Priv. 2014;

23. Mcgettrick A. Toward effective cybersecurity education. IEEE Secur Priv. 2013;

24. Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. Ethical hacking: The need for cyber security. In: IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017. 2018.

25. NortonLifeLock employee. Black Hat, White Hat & Grey Hat Hackers - Differences Explained. NortonLifeLock. 2017.