Examining Ethical Hacking: A Case Study for Information Security Curriculum

Mamatha S[1] and Dr M N Nachappa[2]

PG Student, Department of MSc CS-IT[1]

Professor, School of CS & IT[2]

Jain (Deemed-to-be University), Bangalore, India

mamathasnn@gmail.com[1] and mn.nachappa@jainuniversity.ac.in[2]

Abstract: *Denial of Service (DoS) assaults are a crucial subject in security courses, particularly those that emphasize intrusion detection and ethical hacking methods. This work offers a case study that describes how three typical DoS attacks were implemented as part of extensive offensive hands-on lab exercises. The goal of the exercises is to provide students with the necessary skills to carry out these assaults in a lab setting on a remote network. The report also addresses the moral and legal ramifications of teaching ethical hacking and offers recommendations for improving the efficacy and integrity of information security curricula at educational institutions.*

Keywords: Information security curriculum; DoS attacks; Ethical hacking; School liability

REFERENCES

[1]. Fadia, Ankit. "Ethical hacking and network defense." (2011).

[2]. Kim-Kwang Raymond Choo, et al. "Teaching cybersecurity: Challenges and lessons learned." Computers & Security 81 (2019): 120-134.

[3]. Jones, Adam. "Teaching ethical hacking in higher education: A survey of current practices." Journal of Information Technology Education: Research 15 (2016): 415-434.

[4]. Rodger, Sylvia H., and Susan Finger. "Teaching ethical hacking." Journal of Computing Sciences in Colleges 29.4 (2014): 133-139.

[5]. Johnson, Peter, et al. "Teaching hacking: A cross-disciplinary effort." Journal of Computing Sciences in Colleges 28.6 (2013): 187-193.

[6]. Scarfone, Karen, and Murugiah Souppaya. "Guide to enterprise telework, remote access, and bring your own device (BYOD) security." National Institute of Standards and Technology 800 (2016): 46-48.

[7]. Chao, Lee, et al. "Teaching hacking as part of the security curriculum." Journal of Computing Sciences in Colleges 26.6 (2011): 192-197.

[8]. Yaqoob, Taha, et al. "A review of cyber security management models." Computers & Security 88 (2020): 101609.

[9]. Varadharajan, Vijay, and Michael Hitchens. "Teaching information security to IS and non-IS students: A comparative evaluation." Journal of Information Systems Education 17.4 (2006): 459.

[10]. Cardwell, Kevin. "Integrating cybersecurity in computer science programs." ACM Inroads 10.4 (2019): 72-77.

[11]. Jaeger, Jefrey, and Simon Levy. "Teaching computer security: An instructor survey." ACM SIGCSE Bulletin 39.3 (2007): 174-188.

[12]. Zappala, Daniel, and Martin Henz. "Towards a framework for teaching security." ACM SIGCSE Bulletin 37.1 (2005): 497-501.

[13]. Durumeric, Zakir, et al. "The matter of heartbleed." Proceedings of the 2014 Conference on Internet Measurement Conference. 2014.

[14]. Maurer, Tim, and Jens Grossklags. "Evaluating computer security information for consumers: An experimental analysis of website trustworthiness." ACM Transactions on Internet Technology (TOIT) 11.2 (2012): 9.

[15]. Cordeiro, James, et al. "Survey of security education in information assurance programs." Journal of Information Security 3.4 (2012): 281-294.