Round	14
Grant #	M87
Applicant Name	Hossain Shahriar
Applicant Position	Associate Professor of IT
Applicant Institution	Kennesaw State University
Applicant Email Address	hshahria@kennesaw.edu
Other Team Members	Chi Zhang, czhang4@kennesaw.edu
Type of Project	Creation of ancillaries for pre-existing OER
Course Number(s) and Title(s)	IT 6843, Ethical Hacking & Networking Security
Final Semester of the Project	Summer 2020
Proposed Grant Funding Amount:	$4,800.00
Currently-Existing Resource(s) to be Revised / Ancillaries Created	IT 6843- Ethical Hacking: Network Security and Penetration Testing http://ksuweb.kennesaw.edu/~speltsve/files/ALG_EH_Document.htm
Project Description	(a) Project Description: In this project, we aim to develop hands-on labs for update two existing modules of Ethical Hacking & Networking Security (IT6843) course: IoT and Security Devices. The course was developed as part of ALG Round8 (Grant#302) during early 2017. Over the last few years, there has been considerable progress in both hacking techniques and available tools to detect hacking activities. For example, within IoT security, deep packet inspection is needed to identify malicious traffic, whereas, host computers if compromised through rootkit, firewall/Intrusion Detection System devices won't be effective. In this project, we plan to to develop additional resources for the two existing modules of the course - IoT and Security Devices. In particular, (i) IoT malware: we plan to build a hands-on lab for malware analysis using deep packet inspection with open source tools including Burpsuite [1], Tor [2], Wireshark [3]. The lab will be using Raspberry pi [4] (with Kali Linux [5]). Learners will be able to inspect malware traffic generated through real-world ransomware application. The developed resources will be added into module11 (IoT security). (ii) Security Device: we plan to develop a hands-on lab to detect rootkit within operating systems using two open source tools - chrootkit [6] and RootkitHunter [7].

	The developed resources will be plugged into module 12 (security devices). We are planning to develop the resources based on available documentation of tools, websites, blogs, resources from Youtube, and trial/error run of the tools. b) Project Deliverable: The outcome will be hands-on lab instructions for the two modules. Each lab will provide detailed hands-on instructions showing how to install, configure and apply tools in Kali Linux, gather information for attacks and mitigation. The materials will include learning resources (prelab, hands-on lab) and detailed steps with screenshots so learners are able to replicate the lab on their own computers for advanced learning and research project. References [1] Burp suite, https://portswigger.net/burp [2] Tor browser, https://www.torproject.org/download/ [3] Wireshark, https://www.wireshark.org/ [4] Raspberry pi, https://www.raspberrypi.org/ [5] Kali Linux, 2018, https://www.kali.org/ [6]chkrootkit, http://www.chkrootkit.org/ [7]Rootkit Hunter, http://www.rootkit.nl/projects/rootkit_hunter.html
Timeline and Personnel	6/1/2019 – 9/30/2019: Development of resources - IoT malware (Dr. Shahriar) 10/1/2019 – 12/31/2019: Development of resources - Rootkit (Dr. Zhang) 1/1/2020 – 4/30/2020: Course Teaching and gather feedback (Dr. Shahriar) 5/1/2020 – 6/30/2020: Update resources based on feedback (Dr. Shahriar, Zhang) 7/1/2020 - 8/15/2020: Host materials into website, submit final report (Dr. Shahriar)
Budget	Dr. Hossain Shahriar – $2000 Dr. Chi Zhang - $2000 Travel/Equipment - $800. Total $4800
Creative Commons Terms	I understand that any new materials or revisions created with ALG funding will, by default, be made available to the public under a Creative Commons Attribution License (CC-BY), with exceptions for modifications of pre-existing resources with a more restrictive license.