Lei Li, Zhigang Li, Hossain Shahriar, Rebecca Rutherfoord,
Svetlana Peltsverger, and Dawn Tatum

Ethical Hacking: Network Security and Penetration Testing

Initial Proposal

Application Details

Manage Application: ALG Textbook Transformation Grants Round 8

Award Cycle:	Round 8
Internal Submission Deadline:	Sunday, December 11, 2016
Application Title:	302
Application ID:	#001299
Submitter First Name:	Lei
Submitter Last Name:	Li
Submitter Title:	Associate Professor
Submitter Email Address:	lli13@kennesaw.edu
Submitter Phone Number:	470-578-3915
Submitter Campus Role:	Proposal Investigator (Primary or additional)
Applicant First Name:	Lei
Applicant Last Name:	Li
Co-Applicant Name(s):	--
Applicant Email Address:	lli13@kennesaw.edu
Applicant Phone Number:	470-578-3915
Primary Appointment Title:	Associate Professor
Institution Name(s):	Kennesaw State University
Submission Date:	Monday, December 12, 2016

Team Members (Name, Title, Department, Institutions if different, and email address for each):

Zhigang Li, Instructional Technology Specialist & Part-Time Assistant Professor of Information Technology, zli8@kennesaw.edu
Lei Li, Associate Professor of Information Technology, li_lei@kennesaw.edu
Hossain Shahriar, Assistant Professor of Information Technology, hshahria@kennesaw.edu
Rebecca Rutherfoord, Interim Assistant Dean of the College of Computing and Software Engineering, Chair of the Department of Information technology, and Professor of Information Technology, brutherf@kennesaw.edu
Svetlana Peltsverger, Interim Associate Dean in the College of Computing and Software Engineering and Associate Professor of Information Technology, speltsve@kennesaw.edu
Dawn Tatum, Lecturer of Information Technology, dtatum7@kennesaw.edu

Sponsor, (Name, Title, Department, Institution):

Department of Information Technology

College of Computing and Software Engineering

Kennesaw State University

Proposal Title: 302

Course Names, Course Numbers and Semesters Offered:

IT 6843 - Ethical Hacking: Network Security and Penetration Testing – Offered twice a year in summer & fall semesters.
IT 6833 - Wireless Security– Offered once a year in spring semesters. It's also offer in summer semesters when needed.
IT 6883 - Infrastructure Defense – Offered once a year in fall semesters.
CSE 3801 **-** Professional Practices and Ethics– Offered three times a year in spring, summer & fall semesters with multiple sections each semester

Average Number of Students per Course Section: 34

Number of Course Sections Affected by Implementation in Academic Year: 25

Total Number of Students Affected by Implementation in Academic Year: 855

List the original course materials for students (including title, whether optional or required, & cost for each item):	1. IT4843, Hands-On Ethical Hacking and Network Defense, 2nd Edition, by Michael T. Simpson, Kent Backman, James Corley, ISBN-13: 978-1435486096, 2011. Required. Cost: $202.30, enrollment:50, total cost: $10,115.00 2. IT6843,1) Hands-On Ethical Hacking and Network Defense, 2nd Edition, 2011, by Michael T. Simpson, Kent Backman, James Corley, ISBN-13: 978-1435486096.2) Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition, 2011, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, McGraw Hill, ISBN-13: 978-0071742559. Required. Cost: 1) $202.30;2) $34.90, Total: 237.20, enrollment: 75, total cost: $17,790.00 3. IT6833, Praphul Chandra, 2005, Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security, Publisher: ELSEVIER, ISBN: 0-7506-7746-5. Required. Cost: $74.95, enrollment: 40, total cost: $2,998.00 4. IT6883, 1) Business Data Communications Infrastructure, Networking and Security (Edition 7th, 2012), William Stallings, Thomas Case, ISBN-10: 0-13-302389-3 ISBN-13: 978-0-13-302389-3; 2) Chained Exploits: Advanced Hacking Attacks From Start to Finish (Edition: 1st, 2009), Andrew Whitaker, Keatron Evans, Jack Voth, ISBN-13: 978-0321498816. Required. Cost: 1)$161.70, 2). $45.29, Total: $206.99, enrollment: 40, total cost: $8,279.60 5. CSE3801, A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology, 4th Ed., 2012, by Sara Baase, ISBN-13: 978-0132492676, Required. Cost: $115.70, enrollment: 680, total cost: $78,676.00.
Requested Amount of Funding:	$30,000
Original per Student Cost:	$836.94
Post-Proposal Projected Student Cost:	$0
Projected Per Student Savings:	$836.94

Projected Total Annual Student Savings:	$117,843.60

Creation and Hosting Platforms Used ("n/a" if none):

Kennesaw State University D2L Brightspace

Proposal Category:	No-Cost-to-Students Learning Materials
Final Semester of Instruction:	Fall 2017

Project Goals:

In this project, we propose to take a department-wide effort to transform the five information security related courses using no-cost-to-students learning material. This project not only aims to reduce the financial burden imposed by high cost of textbooks, but also strives to develop free and open-access learning materials that offer equivalent or better educational effectiveness than traditional textbooks. We also plan to develop online offerings of proposed courses that meet the internationally recognized Quality Matters (QM) standards.

Statement of Transformation:

1. The Transformation Description

According to Priceonomics (http://priceonomics.com/which-major-has-the-most-expensive-textbooks/) an average undergraduate student annually spends $1,200 on textbooks. The price of textbooks is now leading students’ course decisions (M. Parry, “Students Get Savvier About Textbook Buying,” The Chronicle of Higher Education, 27-Jan-2013.). The cost of textbooks depends on the major, with computing textbooks being in the top most expensive, and, at the same time, having one of the smallest resale values (Priceonomics). This is more than true for textbooks in Cybersecurity. The content of Cybersecurity courses is constantly changing with various innovations, updates, and revisions needed to keep the information current. Textbook publishers cannot keep up with the fast-moving changes in Cybersecurity and the textbook price for Cybersecurity is very high.

Georgia was recently ranked 3rd in the nation for information security, home to more than 115 information security-related companies (Technology Association of Georgia). Furthermore, there is a significant shortage of trained cybersecurity professionals anticipated in Georgia (USG Cyber Education Committee, 2015). In 2014, Georgia had an estimated 8000 open positions in cybersecurity-related fields with additional shortfalls expected in future years (USG Board of Regents Meeting Minutes, 2015). USG does not produce enough graduates for Georgia's job market. One of the reasons is the cost of education including textbook costs.

The textbooks currently used in the five proposed security related IT courses are quite expensive. Some textbooks do not have the latest edition in the market available (e.g., IT 6833 textbook is from 2005) or, not frequently updated (IT 4843 is from 2011 with new edition just released at the end of 2016 http://www.cengage.com/search/productOverview.do?N=16+4294922389&Ntk=P_EPI&Ntt=15299614671691324142564844329453982650&Ntx=mode%2Bmatchallpartial). The goal of our transformation is to replace the textbook used in the proposed courses with no-cost-to-students learning materials that offer equal or higher educational effectiveness and can be easily updated more frequently.

Four out of six team members were part of the round two of an "Affordable Learning Textbook Transformation Grant" in 2015 (round two, award #119). They designed and evaluated the effectiveness of no-cost-to-students learning materials for database courses in IT department, and saved students $110,419. The assessment results showed that the developed free material offered equivalent or better learning experience than the textbooks did. The preliminary results of the grant were published in the Proceedings of Southern Association for Information Systems Conference (SAIS 2016), the final results were published in the Proceedings of the ACM Special Interests Group in IT Education (SIGITE 2016), "Transforming IT Education with No-Cost Learning Materials". They also hosted a panel discussion on no-cost learning material in IT education, at SIGITE in October 2016. The panel attracted a lot of attention among computing faculty. Many colleagues from different states were impressed with the USG initiative and with course material developed by the team. Building on our past success and lessons learned from the prior ALG grant, we will continue our transformation efforts by developing no-cost learning material for five security related courses.

2. The Stakeholders of the Transformation

There are two primary sets of stakeholders for this proposal – the students taking the five security related IT classes (both in-class and online students), and the faculty developing and teaching those courses. The high cost of textbooks puts a large financial burden on students and may become a road block for students' ability to finish their education. Our team of investigators strives to make higher education more affordable to the students. The information security related learning materials are widely available on the World Wide Web today, and some of them have been created by our faculty members. Many of these resources are publicly accessible, free, or with an open license to use. These materials include open and free tutorials, books, videos, labs, software, and services. For example, the majority of the network protocol specifications are published as Request for Comments (RFC) by the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet. Security protocols such as Wi-Fi Protected Access version 2 (WPA2) are part of the IEEE 802.X group of networking protocols and their specifications are freely available on the Internet. IT security courses include hands-on labs where software and tools get updated frequently and current set of textbooks are not at par with the rapid update. These textbooks (see table 2) contain links to tools or websites which may no longer be available or supported for students to access needed information. As soon as a new version of a tool or software package is released, the instructions in a textbook become obsolete. Therefore, we need to include the latest available tools to prepare hands-on labs.

Many of the textbooks become outdated as soon as they are published, while digital delivery of the learning materials makes it easier to keep the content up-to-date. Developing and assembling a set of learning materials for major security-related courses is a unique approach. It will allow us to better align the learning material not only with the outcomes of each course, but also with the outcomes of the Information Technology program.

Compared to traditional textbooks, the open source software and web resources have many benefits: 1) the Web resources are generally free to use; 2) they are constantly being updated and always reflect the latest trends and industrial development; and, 3) the materials from the Web are also more dynamic and interactive. The pitfalls of Web resources are that they are often disorganized and may contain inaccurate information. However, members of our team of investigators are not only subject matter experts in the information security field, but also proficient educators who on average have more than 10 years teaching experience. We will select, organize and integrate resources from the web and transform the information into instructionally sound learning materials for the proposed courses including content that the team members develop themselves. We strongly believe that the new learning materials will offer up-to-date, equivalent or better learning effectiveness compared to the original textbooks. Digital delivery also allows us to add interactive elements into the learning materials. The interactive content will not only engage the students, but also improve their learning experience. It will help to enhance the learning outcomes and learning satisfaction.

3. The Impact of the Transformation

The impact of our transformation efforts will be profound. By our estimates, more than 850 students will benefit from the no-cost learning material each year. Moreover, it has the potential to benefit more students when the proposed Bachelor of Science in Cybersecurity (eMajor) is approved by the Board of Regents.. The goal of eMajor is to reduce the cost of education by using prior learning assessments, lower tuition and potentially no-cost learning materials (https://emajor.usg.edu). The proposed project is expected to save current students $117,843.60 in textbook costs each year (more if the eMajor is approved). Because of the cost savings from not having to buy textbooks, students may be able to take a few more courses each year and graduate sooner. Having a series of security courses adopting no-cost-to-student material not only offers better and more consistent learning experience to students, but also makes our nationally renowned IT programs more affordable. As a result, our IT programs could recruit more students and produce more qualified IT professionals that Georgia needs. Our experience gained in this transformation project could be useful to other programs or departments who want to lower the cost of education to their students. In summary, we believe the proposed project will have a positive impact in students' retention, progression, and graduation at program, department and institution levels. (http://achievingthedream.org/press_release/15982/achieving-the-dream-launches-major-national-initiative-to-help-38-community-colleges-in-13-states-develop-new-degree-programs-using-open-educational-resources , http://affordablelearninggeorgia.org/documents/ALG_Flyer_Sept_2014.4.pdf.

Transformation Action Plan:

With a coordinated effort, our team of investigators plan the following activities to transform all information security related courses to completely use no-cost learning materials:
* Research and identify no cost reading materials for each of the learning modules in each course. The reading list includes both required readings and optional readings. All of these readings will be publicly accessible, free to use, or openly licensed.
* Research and identify no cost materials that can be shared across the courses.
* Develop study guides and lecture notes for students' use to review course content and key learning points.
* Adopt or develop content, assignments, exercises and lab materials that are no cost to students to replace the ones in the textbooks.
* Develop test banks to replace the ones in the textbooks.
* Adopt open source or no-cost-to-student lab ware for students to gain hands-on experience.
* Update the syllabus to include major resources and no cost materials.
* Re-develop the proposed courses in our learning management system, D2L Brightspace, following Quality MattersTM standards

The responsibilities of each investigator is described as follows.

Dr. Lei Li, IT 6833, Project lead; Subject matter expert, course developer and instructor of record of IT 6833.
Dr. Rebecca Rutherfoord, CSE 3801, subject matter expert, course developer and instructor of record for CSE 3801.
Dr. Svetlana Peltsverger, IT 6843, subject matter expert, course developer and instructor of record for IT 6843.
Dr. Hossain Shahriar, subject matter expert, course developer and instructor of record for IT 4843.
Prof. Dawn Tatum, IT 6883, subject matter expert, course developer and instructor of record for IT 6883.
Dr. Zhigang Li, Provide Instructional Design Support to all five proposed courses.

All course design with the no-cost materials will be provided through D2L Brightspace for our students and on the ALG website for the public access.

Quantitative & Qualitative Measures:

The investigators plan to assess the effectiveness of our proposal in two ways - in the middle and at the end of the semester. Qualitatively, we will design a survey and gather inputs from the students after they use the no-cost learning material. Quantitatively, we will compare students' performance data gathered from sections using traditional textbooks and sections using no-cost learning material.

The investigators will collect student performance data such as pass rates from the five proposed courses taught with a textbook by team members between fall 2015 and summer 2016. This data will be used as a baseline for comparison of student performance in courses with alternative no cost material. Our assessment plan can be summarized as follows.

1. Student performance measures. This data is from the overall class performance based on the grading of student works. Metrics include:

* Class average, grades distribution, pass rate for each grading item.

* Overall letter grades distribution, pass rate, withdraw rate, and fail rate.

* Percentage of students meeting or exceeding learning outcomes

2. Specific survey on no-cost learning materials. A web-based survey will be developed for all proposed courses and be distributed at the end of the semester to collect student feedback. It consists of a mixture of quantitative and qualitative measures including:

* Student perception and attitude toward no cost materials

* Quantitative ratings of the no cost materials used in this course

* Qualitative comments and suggestions

3. Student evaluation of the instructor. Formal student evaluation of the instructor can also provide information about teaching effectiveness using no cost materials. This evaluation is based on standardized forms for every course.For each of the measurement, the investigators are going to conduct two levels of analysis: 1) Comparing the achievement levels of the course learning

outcomes - generally, 75% is the aimed passing rate in undergraduate courses and 80% in graduate courses. 2) Comparing the achievement levels to those from past offerings where costly textbooks were used. The investigators will use the data from the sections taught in the past 2 years.In addition, Kennesaw State University requires all online courses to be reviewed and approved following an internal review process using Quality Matters (QM) standards. This review will ensure the no-cost learning materials used or developed for the cyber security courses are instructionally sound. The College of Computing and Software Engineering will also conduct subject matter expert reviews for all developed courses to ensure the quality of the learning materials.

Timeline:

Spring 2017

* Collect baseline statistics on each course (course developers – those faculty who are in charge of the course for this study)

* Course modules redesigned to use the no cost materials. These include all new content, readings, lecture notes, video clips, exercises, labs, and assignments. The changes are reflected in the learning module study guides. (completed by course developers)

* Course level assessment and informational materials redesign. This includes quizzes, tests, and syllabus. (course developers and instructional designer)

* Submit the developed courses for instructional design review through Quality Matters. (instructional designer and KSU Distance Learning Center office)

* Submit the developed courses for subject matter expert review. (department Chair)

Summer 2017

* Develop a survey on effectiveness of the no cost materials (all course developers and instructional designer)

* Teach:

o IT 6833 - Wireless Security, Dr. Li

o IT 6883 - Infrastructure Defense, Prof. Tatum

* Survey two summer courses and give student course evaluation (course developers and instructional designer)

Fall 2017

* Teach:

o IT 4843 - Ethical Hacking for Effective Defense, Dr. Shahriar

o IT 6843 - Ethical Hacking: Network Security and Penetration Testing, Dr. Peltsverger

o CSE 3801 - Professional Practices and Ethics, Dr. Rutherfoord

* Survey three fall courses and give student course evaluation (course developers and

instructional designer)
* Complete final assessment data analysis and prepare a final report (all course developers and instructional designer)

Budget:

The funding mainly compensates our team of investigator's work and activity beyond normal teaching load or other job responsibilities in order to successfully complete the project. For each proposed course, course developers approximately will spend at least 80 hours in developing the no-cost learning material and be the instructor of record, and, will spend 20 hours in course assessment. Instructional support will devote at a minimum 50 hours in assisting course developers. Thus, we request the budget of this project as follows.

Dr. Lei Li, Project lead; course developer and instructor of record of IT 6833, $5,000
Dr. Rebecca Rutherfoord, course developer and instructor of record for CSE 3801, $5,000
Dr. Svetlana Peltsverger, course developer and instructor of record for IT 6843, $5,000
Dr. Hossain Shahriar, course developer and instructor of record for IT 4843, $5,000
Prof. Dawn Tatum, subject matter expert, course developer and instructor of record for IT 6883, $5000
Dr. Zhigang Li, Provide Instructional Design Support to all five proposed courses, $3,000
Travel: $2,000, for project team members to attend the ALG kickoff and subsequent meetings to bring back information to the team members. Our project team is also planning to submit a paper to reputable IT education conferences such as ACM SIGITE 2017 (Special Interest Group in IT Education).
Total Budget: $30,000

Only open source software or free software will be used in this project thus there is no additional spending on software or equipment purchasing.

Sustainability Plan:

The IT department implemented a course developer system for all courses. A course developer updates course content based on research, publications and feedback from students and alumni. Each of investigators except the instructional designer is a course developer for corresponding course. A course developer creates and maintains the course materials and teaching plans. He/she also teaches the course at least once a year to make sure all resources are valid and makes necessary changes and updates. This makes sure all no-cost materials and resources are highly sustainable in the future offerings of this course.

KENNESAW STATE UNIVERSITY

College of Computing and Software Engineering

Information Technology

August 30, 2016

ALG Grant Committee
University System of GA

Dear Colleagues:

This letter is in support of the Proposal "Transformation at scale: Developing No-Cost-to-Student Information Technology Security Related Courses" submitted from Kennesaw State University, Information Technology department faculty. As Department Chair for Information Technology, I clearly see the need for bringing down costs for our students. The ALG grants assist faculty to prepare no-cost courses that allow students to take courses without the monetary burden of expensive textbooks.

Several faculty in the Information Technology Department at Kennesaw State University have successfully carried out one ALG grant for database courses in the curriculum. The current proposal addresses security related courses in the IT curriculum. The savings already realized from the previous ALG grant encouraged our faculty to develop this new ALG grant proposal to help our students save even more money.

I strongly support this proposal. This is a very sustainable proposal as we have a large Information Technology degree program. Many of our students take courses online as well as in-class. Creating the no-cost for textbook version of our security courses will allow students for many years to realize savings from not buying textbooks for both database and security courses.

This is a very solid proposal. All faculty participating in the first ALG grant completed their courses and offered them successfully. Papers for two conferences about the grant have been created and presented (one this end of September). I believe that this new ALG proposal will have the same student satisfaction and success that the first ALG grant did. This new proposal will have an even larger monetary impact on our students than the first grant. Thank you for your consideration for this proposal.

Sincerely,

Rebecca H Rutherford

Rebecca H. Rutherford, Ed.D.
Interim Assistant Dean of the College of Computing & Software Engineering, Department

Chair for Information Technology, Professor of Information Technology
brutherf@kennesaw.edu

KENNESAW STATE UNIVERSITY

College of Computing and
Software Engineering

December 8, 2016

Dear Affordable Learning Georgia (ALG) Grant Reviewers,

It is my pleasure to write this letter in support of the proposal, “Transformation at scale: Developing No-Cost-to-Student Information Technology Security Related Courses”, submitted by Dr. Li, Dr. Shahriar, Dr. Rutherfoord, Dr. Peltsverger, Dr. Li, and Ms. Tatum from our Information Technology (IT) Department at Kennesaw State University.

In this project, the primary investigators will work as a team to replace existing, costly textbooks in five information security related courses with no-cost-to-students learning materials. Their efforts will significantly lower the cost of education for students (saving over $100k per year at KSU alone) and generate a positive impact on the retention, progression, and graduation for the College of Computing and Software Engineering. Additionally, given the rapid change of the IT field, having digital materials available to students will improve the ability to keep them updated with the latest advances in the field of information security.

Four of the proposers have past experience with a successful ALG project, thus the quality and success of this new project is highly likely. The investigators in this project are also designated course architects who are responsible for the development and the maintenance of the to-be-transformed courses. The no-cost-to-students materials developed will be distributed using the course management system, GeorgiaView Desire2Learn. Thus, I believe the effort of this project will be sustainable over the long term and benefit students throughout Georgia.

In conclusion, I wholeheartedly support this effort. This proposal has the full support of the College of Computing and Software Engineering.

Sincerely,

Jon A Preston

Dr. Jon A. Preston
Interim Dean
College of Computing and Software Engineering
Kennesaw State University

From: Tamara Powell
To: Rachel Myers; Seneca Vaught; Griselda Thomas; John L. Isenhour; John L. Isenhour; Ophelia Santos; Charles Marvil; Shangrong Deng; Laura Ritter; Guangzhi Zheng; Zhigang Li; Lei Li; Rebecca Rutherfoord; Svetlana Peltsverger; Zhigang Li; Nancy Colyar; Ginny Zhan; May H. Gao; Yumin Ao; Carlton Usher; Linda Lyons; Daniel Farr; Tiffani Reardon; Jonathan Arnett; Monique Logan; Cassandra Race; Sharon Pearcey; Chris K. Randall; Jennifer Willard; Beth Kirsner; Adrienne Williamson; Tricia Mahaffey; Chi Zhang
Cc: Rita Spisak; Elke Leeds
Subject: Hello Textbook Transformation Grant Winners! We Would Like to Honor You!
Date: Wednesday, March 2, 2016 1:04:24 PM
Attachments: KSU Library System Authors Request for Items.docx

Hello Textbook Transformation Grant Winners!

You are receiving this email because you have dedicated your time and expertise to reducing the student debt load at KSU. Please see your names and accomplishments listed below. In total, you have reduced at least $1,048,545 from the KSU student debt load each year. Please see the attached and submit your information for the SPSU L.V. Johnson Library Annual Authors Reception. And please let me know if there are any corrections or changes to the information below, as I would like to write up an article celebrating this incredible achievement. Thank you for all your hard work. Tammy

Camille Payne and Rachel Myers (Nursing) student savings, $30,468
Seneca Vaught and Griselda Thomas (AADS) $20,840
John Isenhour, Ophelia Santos, Charles Marvil (Culinary Studies) $13,875
Lake Ritter, Shangrong Deng (Math) $157,865
Guangzhi Zheng and Zhigang Li (Information Technology) $16,833
Lu Kang and Zhigang Li (Chemistry) $184,320
Lei Li, Rebecca Rutherford, Svetlana Peltsverger, Jack Zheng, Zhigang Li, Nancy Colyar (Computer Science/IT) $110,419
Ginny Zhan, May Gao, Yumin Ao (Asian Studies) $11,249
Carlton Usher and Linda Lyons (First Year Studies) $67,250
Daniel Farr and Tiffani Reardon (Sociology) $13,963.80
Tamara Powell, Jonathan Arnett, Monique Logan, Cassandra Race, Tiffani Reardon (DWMA/English) $51,615
Sharon Pearcey, Chris Randall, Jen Willard, Beth Kirsner, Adrienne Williamson, Tricia Mahaffey (Psychology) $345,912
Chi Zhang and Bob Brown (Information Technology) $23,936

--
"My job is not to prop the door of opportunity open. It is to take that door off its hinges once and for all."
Former Massachusetts Lt. Gov. Evelyn Murphy

Dr. Tamara Powell
Director of Distance Education, College of Humanities and Social Sciences
Associate Professor of English
Kennesaw State University
CHSS Dean's Suite, 42 Bartow Avenue NW
MD 2201 Bldg. 22 Rm 5008
Kennesaw, GA 30144-5591
470-578-2911

Syllabus

IT 6843 Ethical Hacking (fall 17)

Dr. Svetlana Peltsverger

IT Department
Kennesaw State University

This course covers the major issues surrounding the use of penetration testing to secure network security and important skills of a professional hacker and common security challenges that an information security officer will face in his/her work. Topics include the ethics of ethical hacking, laws and regulations, vulnerability discovery and risk analysis, internal and external attacks, how malicious hackers attack and exploit system vulnerabilities, penetration testing methods and tools, latest security countermeasures, and various types of penetration testing and programming skills required to complete successful penetration tests and to secure real systems against real attacks.

Course Outcomes

Students who complete this course successfully will be able to

- Differentiate what an ethical hacker can and cannot do legally.
- Evaluate security threats and vulnerabilities.
- Use hacking tools to locate and fix security leaks.
- Assess potential operating systems vulnerabilities.
- Manage and configure network security devices to secure real systems against real attacks.
- In depth knowledge of at least one network security topic.

Module 1 Ethical Hacking Concepts and Pentesting Environment

Introduction and Module Summary

In this module, you will learn ethical hacking concepts and the legal aspect of ethical hacking; specifically, what you can and cannot do legally. Finally, you will build pentesting environment and review basic Linus commands.

Objectives and Outcomes

After completing this module, you will be able:

- Describe the role of an ethical hacker
- Describe what you can do legally as an ethical hacker
- Describe what you cannot do as an ethical hacker
- Run pentesting assignments using Kali and NETinVM virtual machines.

Assigned Reading and Video

1. UNIX commands https://www.math.utah.edu/lab/unix/unix-commands.html
2. Why Cybersecurity Certifications Matter -- Or Not http://www.darkreading.com/careers-and-people/why-cybersecurity-certifications-matter----or-not/d/d-id/1324004
3. Is it Legal to Teach a Course on Computer Hacking? http://writ.news.findlaw.com/ramasastry/20060724.html "in order to know how to combat the enemy, you need to know how the enemy operates."
4. Kevin Poulsen : http://www.nndb.com/people/453/000022387/
5. Georgia Computer Systems Protection Act http://statelaws.findlaw.com/georgia-law/georgia-computer-crimes-laws.html
6. KSU Acceptable Use Policy https://policy.kennesaw.edu/policy/information-technology

Additional Reading and Video

1. The 2016 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Module 2 TCP/IP Concepts

Introduction and Module Summary

In this module, you will review major concepts and aspects of the TCP/IP protocol, including each of the four layers of the protocol stack: Application, Transport, Internet, and Network. You will also review the IP addressing schemes and how they relate to TCP/IP protocol and security

Objectives and Outcomes

After completing this module, you will be able:

- explain the TCP/IP protocol stack
- explain the basic concepts of IP addressing
- use network analyzer
- read a network capture

Assigned Reading and Video

1. TCP state diagram http://commons.wikimedia.org/wiki/File:TCP_state_diagram.png
2. TCP/IP security http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html
3. SOA https://support.dnsimple.com/articles/soa-record/
4. (Video) Wireshark https://www.wireshark.org/#learnWS or http://www.youtube.com/watch?v=UXAHvwouk6Q

Additional Reading and Video

1. TCP Maintenance and Minor Extensions (Active WG) https://tools.ietf.org/wg/tcpm/

Module 3 Network and Computer Attacks

Introduction and Module Summary

In this module, you will learn about different types of malicious software. Malicious software, sometimes referred to as malware, includes viruses, Trojan horses, and worms; different types of malware and network attacks and how to protect their resources from them.

Objectives and Outcomes

After completing this module, you will be able:

- * Describe the different types of malicious software and what damage they can do
- * Describe methods of protecting against malware attacks
- * Describe the types of network attacks
- * Identify different type of attacks and countermeasures

Assigned Reading and Video

1. RSA Phishing Attack http://www.f-secure.com/weblog/archives/00002226.html and linked videos and posts (2011)
2. Qarallax RAT: Spying On US Visa Applicants https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/
3. Billion-dollar Hacker Gang Abuses Google Services To Control Malware http://www.forbes.com/sites/leemathews/2017/01/18/notorious-carbanak-gang-abuses-google-services-to-control-malware/#5aab13774e93
4. IoT Security Flaws Must Be Addressed Immediately, Warns Secure Cloudlink http://www.informationsecuritybuzz.com/articles/iot-security-flaws-must-addressed-immediately-warns-secure-cloudlink/
5. Hackers Stole Data from More than 1 Billion Yahoo User Accounts http://www.toptechnews.com/article/index.php?story_id=132009Y8TWU0
6. (Video) Cyber Hunting the Anatomy of an attack http://go.rackspace.com/brand-deepdives28
7. (Video) Cyber Security: Anatomy of a Main Street Hack https://www.youtube.com/watch?v=ZJ9Q2cAnwnc

Additional Reading and Video

1. Password managers: attacks and defenses https://blog.acolyer.org/2017/02/06/password-managers-attacks-and-defenses/

Module 4 Footprinting and Social Engineering

Introduction and Module Summary

In this module, you will learn about footprinting, a technique used to find network information. A list of several free web tools that can be used for security testers, or attackers, for footprinting is provided. You will also learn how to gather more information when footprinting a network using DNS. and social engineering. Social engineers target the human resources of a network to find its vulnerabilities or perpetrate an attack.

Objectives and Outcomes

After completing this module, you will be able:

- Use Web tools for footprinting
- Conduct competitive intelligence
- Describe DNS zone transfers
- Identify the types of social engineering

Assigned Reading and Video

1. Social Engineering http://info.microsoft.com/rs/157-GQE-382/images/CO-EN-CNTNT-SocialEngineering-weakest%20link.pdf
2. Social engineering http://www.social-engineer.org/framework/general-discussion/
   a. General Discussion
   b. Information Gathering
   c. Psychological Principles
   d. Influencing Others
   e. Attack Vectors
   f. Social Engineering Tools
3. Dnsenum http://tools.kali.org/information-gathering/dnsenum and (video) https://www.youtube.com/embed/8EzrvuatXC8
4. Self-Service Password Reset & Social Engineering: A Match Made In Hell http://www.darkreading.com/endpoint/self-service-password-reset-and-social-engineering-a-match-made-in-hell/a/d-id/1325891
5. (Video) Defcon 21 - Social Engineering: The Gentleman Thief https://www.youtube.com/watch?v=1kkOKvPrdZ4

6. (Video Very Funny) What is Your Password? https://www.youtube.com/watch?v=opRMrEfAIiI&t=6s

Additional Reading and Video

1. Social engineering 101: 18 ways to hack a human [Infographic] http://www.networkworld.com/article/3047484/security/social-engineering-101-18-ways-to-hack-a-human-infographic.html

Module 5 Port Scan

Introduction and Module Summary

In this module, you will learn about different type of port scanning and various tools used for port scanning.

Objectives and Outcomes

After completing this module, you will be able:

* Describe different types of port scans

* Describe various port-scanning tools

Assigned Reading and Video

1. TCP Connection termination http://www.tcpipguide.com/free/t_TCPConnectionTermination.htm

2. Stealth Port Scanning Methods https://www.giac.org/paper/gsec/1985/stealth-port-scanning-methods/103446

3. NMAP tutorial http://nmap.org/bennieston-tutorial/

4. NMAP Cheat Sheet https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

5. DNS Resource records http://www.cisco.com/c/en/us/support/docs/ip/domain-name-system-dns/12684-dns-resource.html

6. (Video) Dig and Nslookup https://www.youtube.com/watch?v=CRa8lx0IsDY

Additional Reading and Video

1. NMAP Reference Guide http://nmap.org/book/man.html

Module 6 Enumeration

Introduction and Module Summary

In this module, you will learn how to enumerate systems: obtain information about users, passwords, and shared resources.

Objectives and Outcomes

After completing this module, you will be able:

* Describe the enumeration step of security testing

* Enumerate Windows OS targets

* Enumerate *nix OS targets

Assigned Reading and Video

1. Netstat https://technet.microsoft.com/en-us/library/ff961504(v=ws.11).aspx

2. Net user https://support.microsoft.com/en-us/help/251394/how-to-use-the-net-user-command

3. (Video) Nesus 6 https://www.youtube.com/embed/30qx-SFwRv8?list=PLB6BB6F9582BA2C5D

4. (Video) OpenVas installation https://www.youtube.com/watch?v=ncVFMZqpaxg

5. (Video) Does Windows Defender Offer Enough Protection in Windows 10 https://www.youtube.com/watch?v=LzBtVozt8YU

6. (Video) Announcing Windows Defender Advanced Threat Protection https://www.youtube.com/watch?v=h9xS7mhi1BA

Additional Reading and Video

1. Backdoor to Reset Administrator Password or Add New User in Windows 7 https://www.raymond.cc/blog/backdoor-reset-administrator-password-add-new-user-windows-7/

Module 7 Embedded Systems

Introduction and Module Summary

In this module, you will learn how to identify vulnerabilities in embedded operating systems and how to protect them. The lab covers Linux OS.

Objectives and Outcomes

After completing this module, you will be able:

- Explain what embedded operating systems are and where they are used
- Describe embedded operating systems
- Identify vulnerabilities of embedded operating systems and best practices for protecting them
- Penetrate Linux OS

Assigned Reading and Video

1. How Hackers Will Attack Your Embedded System and What You Can Do About It http://electronics360.globalspec.com/article/5619/how-hackers-will-attack-your-embedded-system-and-what-you-can-do-about-it

2. HIT http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/When-an-attack-means-murder-The-IoT-healthcare-security-vulnerability

3. Cloud IP cameras http://blog.ioactive.com/2016/03/got-15-minutes-to-kill-why-not-root.html

4. Embedded Hardware Hacking 101 - The Belkin Wemo Link https://www.fireeye.com/blog/threat-research/2016/08/embedded_hardwareha.html

Additional Reading and Video

1. (Video and Article) Hackers Remotely Kill a Jeep on the Road https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

2. The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

3. Why Car Hacking Is Nearly Impossible https://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/

4. Hacking Embedded Devices https://www.defcon.org/images/defcon-21/dc-21-presentations/Phorkus-Evilrob/DEFCON-21-Phorkus-Evilrob-Hacking-Embedded-Devices-Bad-things-to-Good-hardware.pdf

Module 8 Vulnerability Disclosure

Introduction and Module Summary

In this module, you will learn why "how to disclose vulnerabilities" has been one of the most widely debated topics in security in a long time.

Objectives and Outcomes

After completing this module, you will be able:

* Explain the term full public disclosure

* Explain the term reasonable disclosure

* Explain the term window of exposure

Assigned Reading and Video

1. Google Outs Windows Vulnerability After Missed Deadline. http://www.tomshardware.com/news/google-windows-vulnerability-missed-deadline,33706.html

2. The FBI couldn't tell Apple what hack it used, even if it wanted to https://qz.com/661934/the-fbi-couldnt-tell-apple-what-hack-it-used-even-if-it-wanted-to/

3. Gogo Inflight WiFi Boosts Security with Bug Bounty Program http://www.eweek.com/security/gogo-inflight-wifi-boosts-security-with-bug-bounty-program.html

4. (Video) Inside the Mind of a Hacker https://www.youtube.com/watch?v=rHHmvISw6e8

5. (Video) Why Western Union Utilizes a Crowd for Application Security Testing https://www.youtube.com/watch?v=F2laMpUdycM

Additional Reading and Video

1. Bugcrowd program https://bugcrowd.com/list-of-bug-bounty-programs

2. Understanding Responsible Disclosures https://snyk.io/blog/understanding-responsible-disclosures/

Module 9 Compliance and Regulations

Introduction and Module Summary

In this module, you will learn about laws and policies that dictate companies and organizations how to protect information technology, systems and networks from cyber-attacks.

Objectives and Outcomes

After completing this module, you will be able:

* Use a risk management framework

* Show the concept of identity management and how it is important

* Be aware of multiple definitions for the word "policy" within a cybersecurity context

Assigned Reading and Video

1. Federal Information Security Management Act (FISMA) http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act

2. (Video) PCI Breach Scenarios and the Cyber Threat Landscape with Brian Honan: Real World Cyber Attacks and Protecting Credit Card Data https://www.youtube.com/watch?v=57YwoEoqfzQ

3. (Video) Taking the Pain out of PCI Compliance https://www.youtube.com/watch?v=bGesAomMqrY

Additional Reading and Video

1. Risk Management Framework (RMF) https://rmf.org/index.php/what-is-rmf

2. Federal Information Security Management Act (FISMA) https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

Module 10 Hacking Web

Introduction and Module Summary

In this module, you will learn about Web applications and their vulnerabilities. You will also explore several tools used to attack Web servers.

Objectives and Outcomes

After completing this module, you will be able:

- Describe Web applications
- Explain Web application vulnerabilities
- Use the tools used to attack Web servers

Assigned Reading and Video

1. Web Application Security Testing Cheat Sheet https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet
2. Akamai's [state of the internet] / security Q2 2017 report https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf
3. (Video) https://www.youtube.com/watch?v=p658jaPS2Lc

Additional Reading and Video

1. Prepared statements http://ksuweb.kennesaw.edu/~speltsve/eh/prepared_statement.doc
2. Top 10 secure coding practices by CERT https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards
3. OWASP Top 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2017_Release_Candidate_1

Module 11 IoT

Introduction and Module Summary

In this module, you will learn how to protect connected devices and networks in the Internet of things.

Objectives and Outcomes

After completing this module, you will be able:

- * Demonstrate several security issues and challenges of collaborative data acquisition in IoT
- * Illustrate the challenges in securing different IoT applications
- * Express data security management in sensor networks

Assigned Reading and Video

1. A Case Study on Baby Monitor Exposures and Vulnerabilities by Rapid7 https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf
2. IoT Security. http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
3. Why IoT security is so critical https://theiotmagazine.com/why-iot-security-is-so-critical-381f4e7c29fc
4. An Experiment Shows How Quickly The Internet Of Things Can Be Hacked http://www.npr.org/sections/alltechconsidered/2016/11/01/500253637/an-experiment-shows-how-quickly-the-internet-of-things-can-be-hacked
5. IoT Testing Guidelines https://www.owasp.org/index.php/IoT_Testing_Guides

Additional Reading and Video

1. IoT Attack Surface Area https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

Module 12 Security Devices

Introduction and Module Summary

In this module, you will learn about network protection systems that security professionals and network administrators can use to better protect networks. Topics include intrusion detection systems and intrusion prevention systems and their role in network defense, and the concept of honeypots and how they can be usedto better understand the techniques of hackers.

Objectives and Outcomes

After completing this module, you will be able:

* Explain how routers are used as network protection systems

* Describe firewall technology and tools for configuring firewalls and routers

* Describe intrusion detection and prevention systems and Web-filtering technology

* Explain the purpose of honeypots

Assigned Reading and Video

1. (Video) Honeypot https://www.youtube.com/watch?v=fQqWe8br2Gw 35 min

2. (Video) Introduction to Snort https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/128/original/Snort_Rules_Techbyte_Final.mp4?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1509919662&Signature=q8HZ0kcvgK3qxZj3X9k6Gl7RRGA%3D 6 min and https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/125/original/Techbyte_Snort_Final_v2_1080p.mp4?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1509919667&Signature=5s3VyOZgwl6DtC5jlFa0wuxSjM4%3D 7 min

3. (Video) Snort Installation https://www.youtube.com/watch?v=RwWM0srLSg0 30 min

4. (Video) Snort rules https://www.youtube.com/watch?v=RUmYojxy3Xw&t=274s 40 min

Additional Reading and Video

1. Snort User Manual https://www.snort.org/downloads/snortplus/snort_manual.html

2. CVE-2017-5521: Bypassing Authentication on NETGEAR Routers https://www.trustwave.com/Resources/SpiderLabs-Blog/CVE-2017-5521--Bypassing-Authentication-on-NETGEAR-Routers/

Final Report

Affordable Learning Georgia Textbook Transformation Grants

Final Report

Instructions:

A. Your final report submission must include four separate component files:

1. *Completed report form. Please complete per inline instructions. The italicized text is provided for your assistance; please delete the italicized text before submitting your report.*
2. *Course Outline document with links to the materials as used per day, week, or unit, organized chronologically. View Course Outline Example*
   a. *For each resource, give the title, author, Creative Commons licenses (if appropriate), and freely accessible URL to the material. Include all open-access links to all adopted, adapted, and newly created course materials.*
3. *Supporting data on the impact of your Textbook Transformation (survey, analyzed data collected, etc.)*
4. *A photograph of your team and/or your students for use in ALG website and materials.*
   a. *Photograph must be 800x600 pixels at minimum (length x height).*
   b. *Photograph must be taken together: individual team member photographs and website headshots not accepted.*

B. Go to http://affordablelearninggeorgia.org/site/final_report_submission to submit these four components of your final report. Follow the instructions on the webpage for uploading your documents. You will receive a confirmation email. Based on receipt of this report, ALG will process the final payment for your grant. ALG may follow up with additional questions or to request your participation in a publication, presentation, or other event.

Date: 12/12/2017

Grant Number: 302

Institution Name(s): Kennesaw State University

Team Members (Name, Title, Department, Institutions if different, and email address for each):

- Lei Li, Professor of Information Technology, Department of Information Technology, li_lei@kennesaw.edu
- Zhigang Li, Instructional Technology Specialist & Part-Time Assistant Professor of Information Technology, Distance Learning Center, zli8@kennesaw.edu
- Hossain Shahriar, Assistant Professor of Information Technology, Department of Information Technology, hshahria@kennesaw.edu

- Rebecca Rutherfoord, Interim Assistant Dean of the College of Computing and Software Engineering, Chair of the Department of Information technology, and Professor of Information Technology, Department of Information Technology, brutherf@kennesaw.edu
- Svetlana Peltsverger, Interim Associate Dean in the College of Computing and Software Engineering and Professor of Information Technology, Department of Information Technology, speltsve@kennesaw.edu
- Dawn Tatum, Lecturer of Information Technology, Department of Information Technology, dtatum7@kennesaw.edu

Project Lead: Dr. Lei Li

Course Name(s) and Course Numbers:

- IT 4843 - Ethical Hacking for Effective Defense – Offered twice a year in summer & fall semesters.
- IT 6843 - Ethical Hacking: Network Security and Penetration Testing – Offered twice a year in summer & fall semesters.
- IT 6833 - Wireless Security– Offered once a year in spring semester.
- IT 6883 - Infrastructure Defense – Offered once a year in fall semester.
- CSE 3801 - Professional Practices and Ethics– Offered three times a year in spring, summer & fall semesters with multiple sections each semester.

Semester Project Began: Spring 2017

Semester(s) of Implementation: Fall 2017

Average Number of Students Per Course Section:

Number of Course Sections Affected by Implementation:

Total Number of Students Affected by Implementation:

Course	Number of sections	Students in each section	Total Students Affected
IT4843	2	32, 26	58
IT6843	2	7, 17	24
IT6833	2	13, 30	43
IT6883	2	6,20	26
CSE3801	5	48,46,36,35, 63	228
Total	9		379

1. Narrative

A. Describe the key outcomes, whether positive, negative, or interesting, of your project.

Our transformation effort is very successful. In this project, we have transformed five courses using no-cost-to-student learning material. Nine sections and total number of 379 students have been impacted. Students' opinions on Learning material we created are overwhelmingly positive. Our assessment data shows that, in majority of the section where the no-cost learning material were implemented, students' performance is either neutral or better comparing to students' performance in previously taught sections using textbooks.

From the instructors' perspectives, collecting and organizing the learning material ourselves not only enable us to better respond to dynamic nature of the information technology field, but also give us the flexibility to customize the course content to better serve our students. On the other side of the coin, the transformation activities require significant efforts and time commitment from the faculty to collect, organize, create, and maintain no-cost learning material that offers equivalent learning experience as the textbooks. Our transformative efforts in replacing textbooks in the proposed courses will not happen without the strong supports from ALG grant.

With our sustainability plan, the no-cost learning material will be continually used and hundreds and thousands of students from Kennesaw State University will enjoy the cost savings and enhanced learning experience in the future.

B. Describe lessons learned, including any things you would do differently next time.

Below are the lessons learned from the members of our project team.

Dr. Hossain Shahriar on IT 4843. The software tools keep changing fast, for example, wireshark got its latest version recently. Lesson learned is to keep checking on tools for update and revise instructions and screenshots accordingly.

Dr. Svetlana Peltsverger on IT 6843. Some sources I used in class were not available when modules were covered. Most of them were YouTube videos that demonstrated latest attacks. The videos were removed by YouTube. The lesson learned is to use only reputable YouTube channels.

Dr. Becky Rutherfoord on CSE3801. This is the type of course that lends itself well for no textbook. The contents will need to be updated to be sure current issues and ethical links are included for the course.

2. Quotes

Provide three quotes from students evaluating their experience with the no-cost learning materials.

1. "*The presented readings combined with the learning modules was almost always enough for me to gain a solid grasp of the current topic. Whenever more materials were required, the information in the module was at least enough to help me seek out the additional free materials I needed for myself*." -IT6843
2. "*Since we are Information Technology majors, and our assignments are all about technology, textbooks are largely useless. Even in classes that do require textbooks, I never buy them*

because there are so many resources online. It's nice to have sources listed within the course to use in conjunction with what I find on my own. " - IT4843

3. "*I thought this method was far more organized and more readable than an ordinary textbook.*" - CSE3801

3. Quantitative and Qualitative Measures

3a. Overall Measurements

Student Opinion of Materials

Was the overall student opinion about the materials used in the course positive, neutral, or negative?

The overall student opinion about the materials used in the courses is overwhelmingly positive.

Total number of students affected in this project: ____379______

- Positive: ___87.91____ % of _____91___ number of respondents
- Neutral: ___5.49____ % of ___91_____ number of respondents
- Negative: __6.60_____ % of ___91_____ number of respondents

Student Learning Outcomes and Grades

Was the overall comparative impact on student performance in terms of learning outcomes and grades in the semester(s) of implementation over previous semesters positive, neutral, or negative?

We have 5 courses in this project. In term of learning outcomes and grades comparing to previous semesters, three courses are neutral, one course is positive and one course is negative. Overall student performance outcome is neutral comparing to previous semester.

Student outcomes should be described in detail in Section 3b.

Course	**Student Performance outcome comparing to previous semester**
IT4843	Neutral
IT6843	Negative
IT6833	Neutral
IT6883	Neutral
CSE3801	Positive

Choose One:

- ___ Positive: Higher performance outcomes measured over previous semester(s)
- _X__ Neutral: Same performance outcomes over previous semester(s)
- ___ Negative: Lower performance outcomes over previous semester(s)

Student Drop/Fail/Withdraw (DFW) Rates

Was the overall comparative impact on Drop/Fail/Withdraw (DFW) rates in the semester(s) of implementation over previous semesters positive, neutral, or negative?

We have 5 courses in this project. The DFW rates of IT 4843 and CSE 3801 are reduced. The DFW rates of IT 6843 and IT 6833 are slightly increased. Overall, the DFW rates for our project is neutral.

	Drop/Fail/Withdraw Rate:	
Course	Previous semester	Implementation semester
IT4843	2/23=8.6%	1/26= 3.8%
IT6843	4/35=11%	4/24=17%
IT6833	1/31= 3%	2/43 =4.6%
IT6883*		
CSE3801	6/41=15%	6/48=13%

Note: 1) the passing grade for student is B (80%); 2) the DFW rate for IT 6883 isn't available.

Drop/Fail/Withdraw Rate:

___9.22____% of students, out of a total __141___ students affected, dropped/failed/withdrew from the course in the final semester of implementation.

Choose One:

- ___ Positive: This is a lower percentage of students with D/F/W than previous semester(s)
- _X__ Neutral: This is the same percentage of students with D/F/W than previous semester(s)
- ___ Negative: This is a higher percentage of students with D/F/W than previous semester(s)

3b. Narrative

- *In this section, summarize the supporting impact data that you are submitting, including all quantitative and qualitative measures of impact on student success and experience. Include all measures as described in your proposal, along with any measures developed after the proposal submission.*
  In project, we proposed to use multiple channels of data to measure the success of our transformative efforts.
  Quantitatively, we compared students' DFW rates, grades, and success in learning objectives. The DFW rates are taken from student registration system. The student grades and success in learning objectives are assessed Faculty Course Assessment Report (FCAR). Faculty in IT department at Kennesaw State University are required to create a FCAR for every course they teach for each semester. The FCAR includes students' grade and success in achieving the learning outcomes.
  Qualitatively, we developed a survey to collect students' opinion on the learning material used in the courses. Students rated their experience using a 5 points scale. Students also give the opportunities to enter comments they may have. A copy of survey result is attached separately.
  Based on the assessment data we collected, the learning material we created offer the same level of the learning effectiveness as the textbook. Students' performance outcomes and DFW in generally stay the same pre-implementation and post-implementation.

4. Sustainability Plan

The IT department at KSU implemented a course architect system for all courses. A course architect updates course content based on research, publications and feedback from students and alumni. Each of instructor of record is a course architecture for corresponding courses. A course architect develops and maintains the course materials and teaching plans. He/she also teaches the course at least once a year to make sure all resources are valid and make necessary changes. This makes sure all no-cost materials and resources are highly sustainable in the future offerings of this course.

5. Future Plans

- *Describe any impacts or influences this project has had on your thinking about or selection of learning materials in this and other courses that you will teach in the future.*
- *Describe any planned or actual papers, presentations, publications, or other professional activities that you expect to produce that reflect your work on this project.*

Information technology is dynamic field where existing technology frequently get updated and new technology constantly comes out. Due to this reason, the no-cost learning material model naturally fits better for IT curriculum than the traditional textbook models. The faculty in the IT department already completed several individual ALG project and two transform-at-scale grants. The positive feedback from the students and our own development and implementation process inspire more faculty in the IT to get involved with developing no cost learning material for their courses.

We shared our experience from this project in the 14th Annual Open Education Conference in Anaheim CA. Two of our team members, Dr. Rutherfoord and Prof. Tatum hosted a panel discussion on open source learning material in this conference in October 2017. The responses we received from the panel discussion are very positive.

6. Description of Photograph

Left to right: Dr. Rutherfoord, instructor of record; Dr. Li, team lead and instructor of record; and Dr. Peltsverger, instructor of record.