Course Code/Course Title:

FSW108 Deployment and Web Security

Course Description: The Deployment course is an introduction to building and deploying applications to cloud hosting providers. Students will develop a foundational understanding of the benefits and process of deploying a web application to a cloud hosting provider.

Course Length: 40 hours	**Prerequisites:** FSW102		
Course Start Date: **Course End Date:**	**Meeting Days/Times**		

Required Resources:

- 1.8 GHz or faster processor
- 4 GB or more of RAM
- Windows 7, OS X Yosemite or later

Additional Resources:

Students are expected to supply notebooks, pens, pencils, highlighters, folders, ring binders, calculators, USB storage devices and other general supplies as needed to aid in the collection and storage of information in their courses.

A. **For Classes Delivered in an Online Format (for approved courses and campuses).** Online courses are delivered via https://wozu.exeterlms.com in an asynchronous format. Students enrolled in online courses/programs are expected to spend an equivalent amount of time on task, as campus-based students, in meeting course objectives. For Online Courses, the total expected hours required for completion of course objectives are identified on the syllabus as **Total Contact Hours** and reflect the sum of theory, laboratory, and outside hours.

Educational Objectives:

Upon successful completion of this Program, students will be able to:

1. Learn about cloud providers and virtualization
2. Understand the process of deploying code to a remote server
3. Learn how to leverage CI to automate deployments

Course Outline

Web Deployment

Lessons:

1. **Introduction to Deployment:** Includes Cloud Computing, EC2, Amazon Web Services (AWS) Account, Accessing Your AWS Educate Starter Account, Starter Application, Python, Amazon EC2 Instance, AWS Dashboard, EC2 Dashboard, EC2 Creation Process, Instance Dashboard, SSH, Installing the Essentials on EC2, Git, Node.js, MongoDB
2. **Automation:** Includes SCP, Transfer real files, Automation
3. **Travis CI:** Includes Travis CI, Enable Travis CI, Travis CI Deployment Automation, Test Automatic Deployment
4. **VIM and Reverse Proxy:** Includes Vim, Vim Modes, Vim Navigation, Reverse Proxy, Using nginx, Sample Files, Configuring nginx, Route Traffic
5. **Final Project**

Outline:

- **L1 Hands on:** Create a new EC2 instance and deploy the todo-list application as performed in this lesson.
- **L2 Hands on:** Using the `todo-list` project, transfer it to your running EC2 instance. Then, add the deploy scripts to automate deployment with a one-line command.
- **L3 Hands on:** Using the todo-list project, integrate TravisCI for automatic deployment.
- **L4 Hands on:** Using the todo-list project, add the necessary files to get nginx running.
- **L5 Hands on:** Final Project

Final Project:

Create a new AWS EC2 instance which will clone a web app from GitHub. Then, fork that repository and connect it to Travis CI. Finally, configure Travis CI to automatically deploy the application to EC2, and configure Nginx.

Web Security

Lessons:

1. **Introductions to Web Security:** Includes Security Mindset, Trust Boundaries, Web Topology, Authentication, Wireshark Walkthrough, Seeing other People's Traffic
2. **Application Trust Boundaries:** Includes REST, Trust Boundaries Within an Application, cURL Walkthrough, GitHub, Authentication, Application Attack Vectors, DOS, XSS, SQL Injection, DevTools and cURL Walkthrough, Security in Development, Development Lab, Cloning a Repository, Public/Private Keys, Linux Permissions, Adding Keys to GitHub
3. **Hosting Options and Security:** Includes Hosting Security, Cloud Hosting, SaaS, IaaS, PaaS, Shared Hosting, What's in a URL, Protocol Vulnerabilities, ARP Spoofing, DNS Spoofing, DKIM Signatures, Operating System Vulnerabilities
4. **System Administration:** Includes Operating Systems, User Accounts, Applications, Permissions, Ports, Firewalls, Updates, Backups, Audits, PCI DSS, HIPAA, NIST Cybersecurity Framework, Cloud Compliance, Encoding, Hashing, Encryption, Public/Private Key
5. **Internal Attack Vectors:** Includes When Users Attack, Two Factor Authentication, Device Fingerprinting, Customer Fraud, Employee Fraud, Phishing, Security Community, Software Vulnerability Databases, Malware Blacklists, Breach Reports, Trends and Strategic Context, Stages of a Hack

Outline:

- **L3 Hands on:** Using sources on the web to research recent software vulnerabilities. Compile the links you have to these resources into a document and submit it.
- **L4 Hands on:** Create an emergency checklist based on the technologies with which you are working.
- **L5 Hands on:** Final Project
- **Exam:** Web Security Exam

Final Project:

Develop a checklist for system emergencies. For each scenario, make sure to include specific instructions on how to respond for the chosen set of technologies.