C S 55D: SECURITY IN AMAZON WEB SERVICES

Foothill College Course Outline of Record

Heading	Value
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 55A.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- A successful student will be able to identify the role the Key Management Service and the best practices used in deployments.
- A successful student will be able to identify important security principles that web services applications must meet when deployed.
- A successful student will be able to describe use of the Shared Responsibility model in secure AWS deployments.

Description

This course focuses on protecting the confidentiality, integrity and availability of computing systems and data. Students learn how Amazon Web Service (AWS) uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure the underlying infrastructure is continuously monitored and protected. Students examine the AWS Shared Responsibility Model and access the AWS Management Console to learn more about security tools and features provided by the AWS platform.

Course Objectives

The student will be able to:
A. Apply for an Amazon (AWS) account and Amazon Educate account
B. Demonstrate the basics of the AWS Security and Compliance Principles
C. Understand and describe the Shared Responsibility model and AWS configuration
D. Configure the AWS Identity Access Management (IAM) system
E. Use the AWS CloudTrail and CloudWatch services
F. Understand Inspector and Trusted Advisor services
G. Configure AWS Virtual Private Cloud (VPC) and Route 53 (DNS) services
H. Understand principles of AWS CloudFront (content distribution), WAF (web access firewall) and Shield services (DDoS protection)
I. Demonstrate the Key Management Service and use best practices

Course Content

A. AWS access
1. AWS account acquisition
2. AWS command line interface
3. AWS Educate account acquisition
B. Introduction to AWS Security and Compliance Principles
1. Shared responsibility model
2. AWS security responsibilities
3. Customer security responsibilities
4. AWS Compliance Program standards and practices
5. Physical and environmental security
6. Business continuity management
7. Network security
8. AWS account security features
C. Shared Responsibility Model and AWS configuration
1. AWS Secure Global Infrastructure
2. Using the AWS Identity and Access Management service (IAM)
3. Review AWS regions, availability zones and endpoints
4. Security basics for:
a. Infrastructure services (EC2 compute, EBS block store, VPC virtual private cloud)
b. Container services
c. Abstracted services (S3 data, database, queuing)
5. AWS configuration principles
a. AWS configuration review
b. Resource administration
c. Auditing and compliance
d. Change management and troubleshooting
e. Security analysis
D. Identity Access Management (IAM)
1. IAM features
2. IAM principles
a. Principal
b. Request
c. Authentication
d. Authorization
e. Actions
f. Resources
3. IAM users
4. Permissions and policies
5. Practical IAM usages
a. Assigning users
b. IAM administration of users and groups
c. IAM command line interface
d. IAM multi-factor authentication
E. AWS CloudTrail and CloudWatch fundamentals
1. CloudTrail concepts (governance, compliance, operational/risk auditing)
a. CloudTrail fundamentals
b. Workflow
c. Regions
d. Log files
2. CloudWatch concepts
a. Monitoring
b. Access methods
c. Related AWS services
d. Principles of operation
e. More concepts
1) Namespaces
2) Metrics
3) Dimensions
4) Statistics
5) Percentiles
6) Alarms
3. Setup and usage
F. Inspector and Trusted Advisor
1. Inspector concepts and fundamentals

a. Analysis of behavior of AWS resources security issues
b. Basic features
c. Pricing
d. Access methods
e. Terminology and concepts
f. Service limits
g. Regions and platforms
h. Setup
i. Assessment targets and instance tags
j. Inspector agent
1) Walk through with Ubuntu Server
2) Agent privileges
3) Agent security
4) Agent updates
5) Access control
2. Trusted Advisor best practices checks
a. Cost optimization
b. Fault tolerance
c. Service limits
d. Security
e. Performance
G. Virtual Private Cloud (VPC) and Route 53 (DNS)
1. VPC fundamentals
a. Virtual private clouds and subnets
b. Default and non-default VPCs
c. Internet access
d. Tunneling access
e. AWS PrivateLink
f. VPC with other Amazon Services
g. Access methods
h. Launching VPC
1) VPC creation
2) Security group creation
3) Launching Instances into the VPC
i. Scenarios and examples of VPCs
2. Route 53 fundamentals
a. Domain registration
b. DNS service
c. Health checking
d. Routing and resource sets
H. CloudFront, WAF and Shield Services
1. CloudFront
a. Principles of operation
b. Setup
c. Use cases
d. Locations and IP addressing
e. Access control lists
2. WAF and Shield Services
a. DDOS review and attack types
b. AWS DDoS response team
c. Use cases
I. Key Management and best practices
1. Customer master keys
2. Data keys
3. Envelope encryption
4. Encryption context
5. Key policies
6. Grants
7. Grant tokens
8. Auditing CMK usage
9. Key Management Infrastructure
10. Key usage
a. Key creation
b. Viewing keys
11. Best practices overview

Lab Content

A. Create necessary AWS accounts
B. Configure AWS Config to monitor all AWS resources in your region
C. Establish an IAM group for managing your sites
D. Enable CloudTrail by creating a trail and configuring it to record all API call from all AWS regions
E. Establish a CloudWatch Billing Alarm, setup an alarm to trip when your billing reaches $100.00 and have the alarm signaled by an SMS message
F. Establish a CloudWatch Event Rule to monitor EC2 instance state changes resulting in termination of the instance
G. Launch an Amazon Linux instance and install and configure Linux Inspector
H. Configure Trusted Advisor to monitor security events
I. Configure a Virtual Private Cloud (VPC) instance with public and private subnets and launch an EC2 instance in each subnet
J. Setting up an instance of the AWS Web Application Firewall (WAF) protection against common attacks
1. Protect against:
a. Cross-site scripting attacks
b. SQL injection attacks
c. Attacks from known bad IP addresses
2. Associate your WAF ACL to your CloudFront Distribution
K. Setup the pre-configured WAF ACL, rules and conditions for Lambda provided by AWS

Special Facilities and/or Equipment

A. Access to a computer laboratory with web browsers.
B. Website or course management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on campus (i.e., face-to-face) offerings.
C. When taught via Foothill Global Access on the internet, the college will provide a fully functional and maintained course management system through which the instructor and students can interact.
D. When taught via Foothill Global Access on the internet, students must have currently existing email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

Methods of Evaluation may include but are not limited to the following:

A. Tests and quizzes
B. Written laboratory assignments, which include detailed instructions, sample runs and documentation
C. Final examination

Method(s) of Instruction

Methods of Instruction may include but are not limited to the following:

A. Lectures which include motivation for the architecture of the specific topics being discussed.
B. In-person or online labs (for all sections, including those meeting face-to-face/on campus), consisting of:

1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work.
2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members.
C. Detailed review of laboratory assignments which includes model solutions and specific comments on the student submissions.
D. In person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing and analyzing programs.
E. When course is taught fully online:
1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment.
2. Additional instructional guidelines for this course are listed in the attached addendum of C S department online practices.

Representative Text(s) and Other Materials

Anthony, Albert. Mastering AWS Security: Create and Maintain a Secure Cloud Ecosystem. Packt Publishing, 2017. ISBN-13: 9781788293723.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

A. Reading:
1. Textbook assigned reading averaging 30 pages per week.
2. Reading the supplied handouts and modules averaging 10 pages per week.
3. Reading online resources as directed by instructor though links pertinent to programming.
4. Reading library and reference material directed by instructor through course handouts.
B. Writing:
1. Writing technical prose documentation that supports and describes the assignment that are submitted for grades.

Discipline(s)

Computer Science