Resources/Links/Tools

Module 1

- AWS Security Best Practices: Cloud Security Report 2020 for InfoSec
- Cloud Security Alliance Controls Matrix
- CSA Security Guidance for Critical Areas of Focus in Cloud Computing
- NIST SP 500-292

Module 2

- Docker security | Docker Documentation
- Trusted Computing Group
- OWASP Serverless Top 10 | OWASP Foundation
- How to Survive 4 Cloud Horror Story Scenarios
- OWASP/www-project-zap: OWASP Zed Attack Proxy project landing page.
- osrframework/INSTALL.md at master · i3visio/osrframework
- Privacy is sexy - Enforce privacy & security on Windows and macOS
- Sysdig | Security Tools for Containers, Kubernetes, & Cloud
- Pacu: The Open Source AWS Exploitation Framework - Rhino Security Labs
- cr0hn/dockerscan: Docker security analysis & hacking tools
- S3Scanner
- Pentesting AWS in the Cloud
- CloudGoat Vulnerable by Design
- 3 Essential Steps to Securing Your Docker Container Deployments

Study Questions

1. Salesforce CRM and Microsoft 365 are two examples of which cloud computing service type? a. IaaS b. PaaS c. SaaS d. Public
2. Which cloud offering relies on the customer having the most responsibilty? a. SaaS b. PaaS c. IaaS d. Public
3. Which of these might be a concern when moving services to a cloud provider? a. Multiple user accounts b. Lack of Transport Layer Encryption c. Lack of fault tolerance in the cloud d. Inability to implement security controls
4. By default, what privilege level does a docker container run at? a. User b. System c. Session d. Root
5. What can be used to audit Docker container a. Docker Hub b. Docker Content Trust c. Docker Bench Security d. Docker swarm

Answers

1. (c) Customer is pay for a subscription based service.
2. (c) IaaS requires the most customer responsibility at they are responsible for everything above the hardware layer.
3. (d) Implementing security controls is a challenge regardless of the platform. Most businesses are less familiar with the cloud than their local networks.

4. (d) Docker contains run as root. To mitigate, you can choose to modify the dockerfile to ensure they all run as a non-root user, or you can run the docker command with the --user [username] paramenter.

```
docker run --user mj ubuntu:latest
```

5. (c) Docker bench security will check host and docker daemon configurations, docker daemon configuration files, container images and build files as well as container run time

Vocabulary

- **Infrastructure as a Service (IaaS)** - cloud servcie provider (CSP) provides and maintains the hardware, power, HVAC and hardware updates, while the customer is responsible for all virtual resources created, including updating those resources at the operating system level.
- **Platform as a Service (PaaS)** - the CSP takes on more responsibility for things such as patching (which customers are historically terrible at and serves as a primary pathway to security incidents) and maintaining operating systems.
- **Software as a Service (SaaS)** - the customer can only make changes within an application's configuration settings, with the control of everything else being left to the CSP (think of Gmail a basic example).
- **Trusted Computing** - Trusted Computing is the simplest method of providing confidence in a platform or computer Trusted Computing enables whoever has an unprotected copy of software or data to state which environment is used to protect that software or data This is the most liberal method of protection