DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK EIGHT/ LESSON ONE

Agenda

- What we've covered
- Tools we've released
- Problems we've encountered
- Capstone Project
- Ideas
- Lab

What We've Covered

- Week 1
  - What is **DevSecOps**?
  - Think like an attacker
- Week 2
  - Intro to Full Stack Development
  - Build a Weak Rails app
- Week 3
  - AWS Basics
  - Intro to AWS Deployments
  - Attack Insecure Apps
- Week 4
  - Getting to know your logs
  - Creating alerts
  - Reports and Dashboards

What We've Covered

- Week 5
  - Infrastructure-as-code
  - Application Availability & Cloudformation
  - End-to-end infrastructure-as-code
- Week 6
  - Offensive security
  - Network Attack
  - AWS IAM Security
- Week 7
  - Gathering forensic data
  - Capturing Forensic images
  - Performing Forensics
- Week 8
  - Wrap-up

Tools We've Released

- https://github.com/devsecops
  - Assumer
    - https://github.com/devsecops/assumer
  - Restacker
    - https://github.com/devsecops/restacker
  - Selfie
    - https://github.com/devsecops/selfie
  - Raindance
    - https://github.com/devsecops/raindance
  - Radar
    - https://github.com/devsecops/radar

Problems We've Encountered

- Bootcamp
  - Vagrant Image
    - Out of sync time
    - Missing tools
    - Deployment/build issues
  - Materials
    - Lab Errors
- Tools
  - Session timeout
  - Bugs

Capstone Project

1. Team up
2. Define the problem
3. Define scope
4. Write use cases
5. Build the capability
6. Get Help

Ideas

1. Vagrant all-in-one DSO image
2. Demonstrate AWS Hologram - https://github.com/AdRoll/hologram
3. Create the DSO CLI – unifies the DevSecOps deployment tools
4. Add forensic configuration data gathering capability to Selfie
5. Add configure feature to Restacker to add/edit target accounts
6. Create/Demo a tool to perform memory forensics in Linux on AWS
7. Add unit testing for CloudFormation to Radar
8. Add attack files/checks to Gauntlt - https://github.com/gauntlt/gauntlt

Lab

1. Register your project as an issue under the GitHub project
    1. Problem
    2. Scope
    3. Use cases
2. Build the capability
3. Get Help