A Cloud Based Entitlement Granting Engine

Daniel Mancini, Austin Cottrill, David Krovich

Lane Department of Computer Science and Electrical Engineering

West Virginia University
COLLEGE OF EDUCATION AND HUMAN SERVICES

Introduction

Cyber Sandbox Software Portal (CSSP) is a web application built on the Ruby on Rails framework which provides an entitlement granting engine to assign AWS Instances to different users on demand. The motivation behind this effort is to create an easy way to give users access to virtual machines while also monitoring their work. CSSP would be useful in a classroom setting that requires students to have their own machines to work on. It would also be useful in training for cybersecurity competitions such as the Mid-Atlantic Collegiate Cyber Defense Competition. By utilizing the cloud and cloud programming API's, virtual instances can be allocated on demand which can not only save a huge amount of time, but also greatly reduce costs of setup, deployment, delegation, and usage of resources.

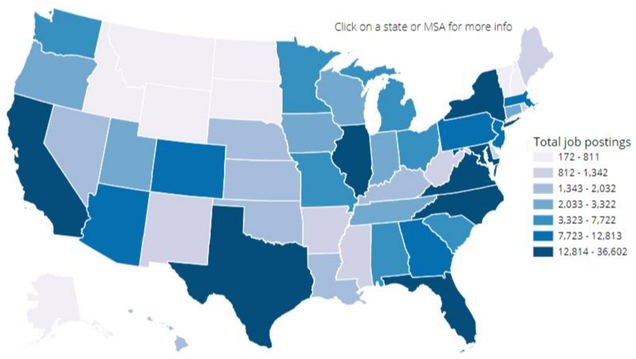
Aim

How can institutions produce more industry ready workers in Cybersecurity?

The need for trained cybersecurity professionals is growing immensely as threats evolve. Reports have shown that unemployment in the industry is effectively zero percent with an estimated shortfall of 1.5 million workers needed. There simply are not enough qualified professionals to meet the demand.

Challenge Based Learning (CBL) methodology can be effective in preparing industry-ready workers to meet the growing demand for qualified cybersecurity professionals. In CBL, participants are presented with problems or challenges where they need to work together in a team environment to come up with a solution. The Mid-Atlantic Collegiate Cyber Defense Competition (MACCDC) is one example of the CBL concept. In this competition, student teams inherit real world environments and attempt to defend them from attack. Teams are also given real world tasks known as "injects" that they must attempt to complete during the competition.

Setting up and configuring these infrastructures to train for MACCDC have all the same problems as setting up infrastructures in the real world. Hardware costs, network concerns, electrical power, and HVAC are a few of the barriers to setting up real world training environments for cybersecurity education.



Map of cybersecurity job postings in the U.S. (taken from cyberseek.org)

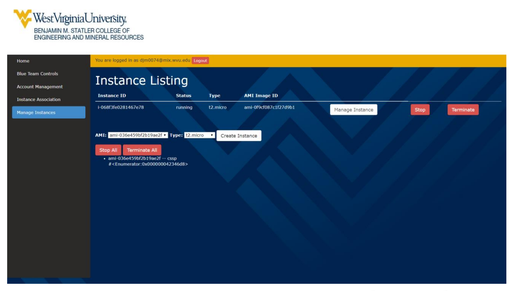
Methods and Functionality

AWS was used for all cloud resources in CSSP. AWS is a leading provider of cloud resources and has a wealth of features and functionality to aid in the construction of a cybersecurity environment. AWS provides several APIs to allow manipulation of cloud resources through many popular programming languages. CSSP is developed in Ruby on Rails so the AWS Ruby API was used.

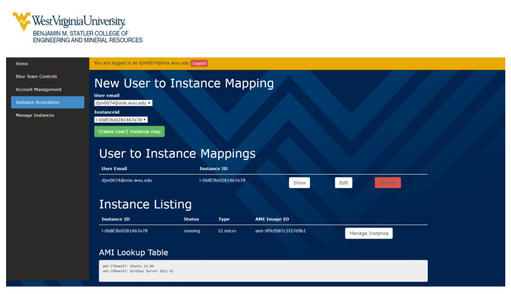
Roles:
The CSSP web application was built with 3 main user roles: Unauthenticated User, Blue Team User, and Administrative User. The Unauthenticated User role has no access to the system, the Blue Team role is meant for students, and the Administrative User role which deals with administrative functions of CSSP.

Identity and Authentication Management:
CSSP relies on the OAuth2 protocol and uses Google as a backend to authenticate users. This allows users to log into the CSSP web application using their Gmail credentials. Once authenticated through Google, a user entry is made in CSSP to track the user through the application. It is during this process that an Unauthenticated User will become either a Blue Team User or an Administrative User.

Deployment:
CSSP is meant to be run from a Docker container. Once a target host is provisioned with Docker, the administrator will clone the CSSP repository from GitHub. Next, several environment variables must be exported on the host including Google OAuth2 and Amazon Web Services credentials. A "build" script and a "run" script are provided which generates the Docker image and launches the container. Then an initial setup script from within the container will be executed which provisions the Virtual Private Cloud (VPC), Access Control Lists (ACL's), subnet security groups, and routing tables within Amazon Web Services. The Ruby on Rails application can now be started from within the container.



Instance Management control panel where the administrator can monitor all active instances.



User to Instance Mapping interface that allows an administrator to associate a user to an instance.

Live Simulation

CSSP was used for the final exam of an upper level cybersecurity course at West Virginia University. The exam required students to inherit the system that was given to them, setup a web server, and hunt for back doors in the virtual instance that they were working in. This exam was designed to test their abilities in Penetration Testing.

Steps taken with OVAs:

1. Create OVA, download it, then upload it to a website for students to access it
2. Each student downloads the OVA and completes the assignment
3. Once they are finished, students create a new OVA, download it, and then upload it to the same website
4. Instructor downloads each and every OVA to grade the work

OVA files are massive 5-20gb files that take a very large amount of time to upload and download.

Steps taken with CSSP:

1. Create custom AMI
2. Create the instance and associate the student to that instance in one click
3. Students SSH into the instance and complete assignment
4. Once the time is up, instructor can stop all instances with one click and grade each one on their own time with ease

This is all that was needed to set up the final exam with the usage of CSSP. No uploading or downloading.

Conclusions

Using CSSP addressed a lot of the concerns with handling assignments that required students to have their own machine as well as providing a training test ground for students to utilize. Giving access to a Windows server or a Linux server becomes a very easy process. Log in as an administrator, click a button, and then associate the newly created instance with a user's Gmail address. The admin can stop or terminate the instance once the user is finished with it. The process can easily scale from a few students to hundreds of students if desired.

Acknowledgments

Dr. Brian Woerner, Dr. Roy Nutter, Dr. Hany Ammar, Mr. Dale Dzielski, Brian Sweeney, Cameron Morris, Brandon Phillips, Michael Petik, Mrs. Cindy Tanner, Dr. Saiph Savage, Mr. Terry Ferrett, Kevin Knopf, Brian Shafer, WVU's RAP Program, and all the students past and present of CyberWVU, WVU's Student Organization that focuses on cybersecurity.