Northeastern University

MSCY Capstone Project Proposal Plan

Wilson: Azure Cloud Lab Chamber

Team Members: Carter Codell, Jason Hewgill, Stephen Neville, Sheetal Singh, Brianna Weinstein

Advisor: Prof. Mardiros Merdinian

Course: CY 7900

2022-01-13

Table of Contents

Table of Contents	**2**
Introduction and Context	**3**
Motivation	**4**
Review of Literature	**5**
Objectives	**7**
Project Approach	**8**
Project Management	**9**
Team Introduction	**10**

Introduction and Context

Our capstone project is Wilson: an Azure cloud lab chamber. Wilson is a platform for quickly building, deploying, and attacking Azure lab environments. Wilson is used as a tool for training cybersecurity professionals who benefit from practice analyzing live cyberattacks in Azure. As cloud technology usage continues to grow in the public and private sectors, malicious actors will have new ways of attacking an organization.

Live experience in a training environment is one of the best ways for a cybersecurity analyst to practice their skills. The most common usage of Wilson is a training manager leading a lab exercise for cybersecurity analysts and incident responders. The training manager uses a template file to build an Azure environment consisting of a network of victim attacker machines. Using scripts and configuration files, the training manager initiates cyberattacks to occur on a regular basis. Next, the training manager gives access to the environment for their students. The analysts and responders learn to detect, report, and stop the attack within a cloud environment.

In addition to training experience for blue team defenders, we believe Wilson has many other applications. A training manager can set up the environment and train red team attackers in attacking the cloud. Business continuity and disaster recovery managers can use Wilson to visualize a cloud cyberattack. Universities and cybersecurity companies can host Azure CTFs using Wilson to set up the infrastructure.

Motivation

As cybersecurity students and professionals, we are always seeking to learn more and improve our skills. While there are many opportunities to build on our knowledge such as TryHackMe, Hack The Box, capture the flag competitions, and blue team competitions, these are all well-structured avenues. There is currently no free, open source platform on Azure for building a custom training environment for cybersecurity professionals. The platform we are proposing would fill this gap in the industry. Users would gain exposure to analyzing live cyberattacks, creating new red team scripts, and implementing security controls. The basic framework will exist for an ever expanding training environment, including fully customizable attacks from the training manager. By allowing this freedom and flexibility, our platform will provide any group of cybersecurity students access to a fully customizable training environment, regardless of the level of their training.

Review of Literature

- *Pentesting Azure Applications: The Definitive Guide to Testing and Securing Deployments.* Written by: **Matt Burrough**
    - This book is a guide to penetration testing Azure cloud services. It covers misconfigurations, enumerating firewall rules, and investigating specialized Azure services. We will use it to draft attack scripts.
- *Microsoft Azure Security Center*. Written by: **Yuri Diogenes** (Microsoft Azure Security Center, First Edition (oreilly.com)
    - This book gives an overview of the Azure framework. It also goes into great detail about the steps needed to secure the Azure cloud services through the process of detecting, investigating, and addressing many different types of threats.
- *Cloud Security Automation: Get to Grips with Automating Your Cloud Security on AWS and OpenStack*. Written by: **Prashant Priyam** (ProQuest Ebook Central - Detail page)
    - This book is a very great overall view of cloud security. It details certain automation techniques that are vital in cloud security, especially with Azure. It will be an important book to help develop blue team scenarios that may use automation to detect security issues.
- *Adaptive evidence collection in the cloud using attack scenarios.* Written by: **Liliana Pasquale** (Adaptive evidence collection in the cloud using attack scenarios - ScienceDirect (neu.edu))
    - This paper details different attack techniques; both inside and outside attacks that could be very useful in the different scenarios that we must develop to confuse our blue team members. It also shows how to collect the evidence from the attacks.
- *Learn Terraform for Cloud Infrastructures***.** Video series by **Niyazi Erodan.** https://learning.oreilly.com/videos/learn-terraform-for/9781838982959/
    - This is a video series that will be a good introduction on building proper, strong, secure terraform code that will be flexible with implementation into cloud environments. Specifically, in this case, it will be used for Azure and building out the environments adequately, as well as setting up our initial terraform development environments.
- *Deep-Dive Terraform on Azure: Automated Delivery and Deployment of Azure Solutions.* Textbook by**: Ritesh Modi**. https://learning.oreilly.com/library/view/deep-dive-terraform-on/9781484273289/
    - This documentation is specifically designed for Azure platform Terraform integration. It covers best practices for IaC and TF, creating reusable scripts and management of security concepts, as well as devops pipelines, as well as modularization of tf components.
- *Jenkins Handbook:* A guide built for the open source software, Jenkins. https://www.jenkins.io/doc/book/

    - This will help us pipeline our environment developments, and help make someone who is specifying environment characteristics' job easier through straight forward deployment and variable choice.
- *Continuously deploy from a Jenkins build.* **Microsoft documentation.** https://docs.microsoft.com/en-us/azure/devops/pipelines/release/integrate-jenkins-pipelines-cicd?view=azure-devops&tabs=yaml (along with other microsoft documentation).
    - This documentation will help us as a group to deploy our infrastructure across multiple subscriptions. It is directly from Microsoft and is documentation regarding DevOps with specific 3rd party pipeline applications. Includes pricing information etc. Information on deployment within azure as well as outside of Azure with just integration / linking.
- *Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security.* Written by: **Marshall Copeland** and **Matthew Jacobs.** https://learning.oreilly.com/library/view/cyber-security-on/9781484265314/
    - An introduction and overview of the various controls in an Azure environment that can be deployed. This will help us determine the difficulty levels of different environments, what security tools we can enable or disable and help to tune the security of our environment for a potential red team / blue team.
- *Learn Azure Sentinel.* Written by: **Richard Diver, Gary Bushey, Jason S. Rader.** https://learning.oreilly.com/library/view/learn-azure-sentinel/9781838980924/
    - This is an important document to understanding azure sentinel, and threat hunting and searching within an environment to detect an attack, and properly combat it using threat analytics and Advanced hunting queries.
- *Cloud Defense Strategies with Azure Sentinel: Hands-on Threat Hunting in Cloud Logs and Services.* Written by: **Marshall Copeland**. https://learning.oreilly.com/library/view/cloud-defense-strategies/9781484271322/
    - Similar to the above, this will help blue teamers understand where they can go to determine if an attack has occurred, how to review what has occurred within their environment, and adequately respond to a threat. It will also help us in determining which styles of breach we would like to occur based on what logs will be determined and with our difficulty assessments.
- *The 7 Deadly Sins of Azure Misconfiguration and How to Fix Them.* Written by: **Microsoft**. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE36QLE#:~:text=By%20far%20the%20most%20common,cloud%20resources%20hosted%20in%20Azure
    - Given that many cloud security breaches occur due to simple misconfigurations, this will be something that we set in several of our templates. It will help the blue team understand the importance of proper configuration and teach them how to correctly configure Azure resources.

Objectives

Our main objective is to deliver a platform for creating Azure cloud training labs. We want to include customizable settings and real-world examples for our users. The sample attack scripts and Azure configuration files should be parameterized to allow the training manager to customize each training session. The examples should be complex enough to have real value beyond a simple tutorial of the trainees' SIEM. Real Azure use cases should be modeled in the templates for the trainees to use. After the training exercise, we want to provide a "lessons learned" opportunity. We will write answer keys that demonstrate how to detect and prevent the attacks simulated in each lab. These answer keys could include: firewall rules, correct configurations of Azure services, or Azure Playbooks to use within Azure Sentinel.

Project Approach

Wilson has three core components: (1) an Azure lab environment consisting of victim and attacker machines; (2) a scenario of automatic cyberattacks using the attacker machines; and (3) a SIEM for analysts to use in the lab.

Building the Environment

Azure has a GUI portal and CLI for building, deploying and managing Azure environments. Ideally, the training manager automatically builds most of the environment and tunes specific parts to customize their trainees' experience. Terraform is an open-source tool that uses the Azure CLI to provision and manage cloud environments. We will write and test Terraform template files that build a variety of Azure environments. To manage scheduled iterations of these templates, we will use Jenkins. For customizability, the training manager can build their Terraform templates or fine-tune our templates using the Azure Portal.

For security from non-participants, the environment will be inaccessible from the public Internet. All of the victim resources and machines will have their own private virtual network within the lab. The attacker machines may be segmented into another private virtual network, depending on the training manager's needs, but they will be inaccessible from the public Internet.

Writing the Scenario

To provide a simulated environment of live attacks, we will use automation tools to replay common and custom cyberattacks. The MITRE ATT&CK Matrix is a great tool for identifying common cyberattacks. We will write scripts in Bash and Powershell that perform attacks and use tools such as cron to replay them. The training manager can tweak our scripts to change attack parameters and can access the attacker machines' shells to perform live cyberattacks. We will write answer keys or playbooks describing how to detect and stop the attacks for the training manager.

Detecting and Stopping the Attack

Azure Sentinel and the ELK stack are two common SIEMs that organizations use to identify cyberattacks. We will provide at least one for trainees to use during the lab. The trainees can write Azure Playbooks to have a better understanding and layout of the cyberattacks that were used during the simulation training.

Project Management

We will use Jira to manage sprint planning and task assignments. Before each sprint we will have a meeting to develop more descriptive and concrete tasks. These tasks will be individually assigned and have a completion timeline.

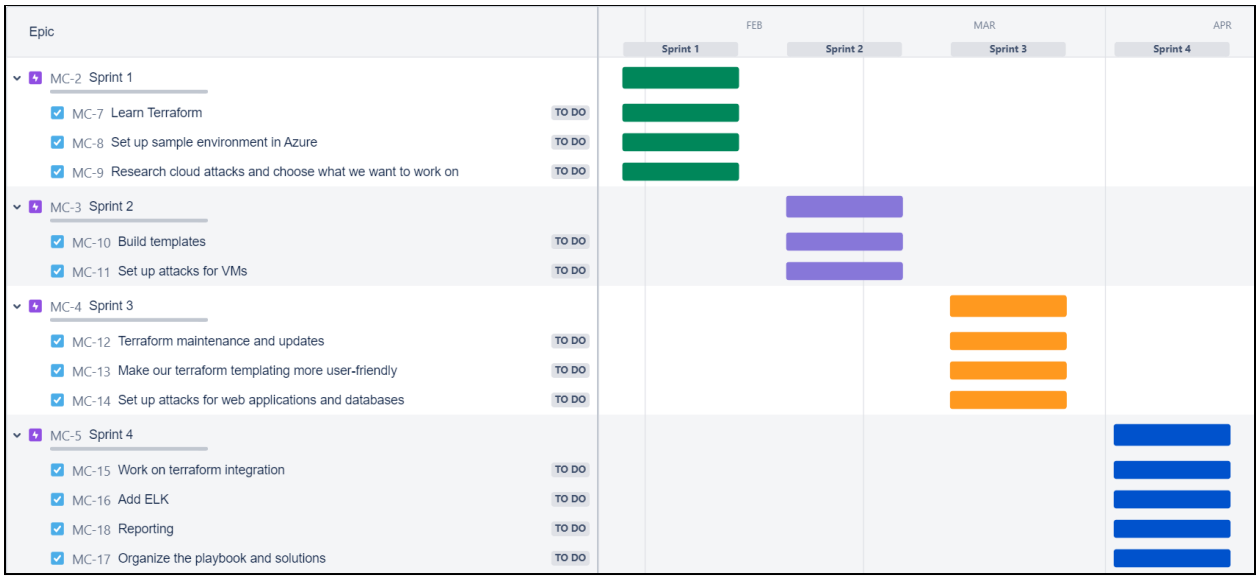

Figure 1: Gantt Chart Export from Jira

Team Introduction

Carter Codell is a student and teaching assistant at Northeastern University and expects to earn his M.S. in Cybersecurity in 2022. He recently finished a cybersecurity internship at the Department of Defense. Carter earned his B.S. in Cybersecurity in 2021, and his undergraduate research project was in Light Weight Encryption for Secure Delay-Tolerant Satellite Networks. The project was through the Information Security Research and Education (INSuRE) project with guidance provided by the National Security Agency. Carter's interests include PCB design, soldering, 3D design, and woodworking. In his freetime, Carter volunteers at Hands to Paws, a local non-profit cat and dog adoption agency.

Jason Hewgill is a student at Northeastern University and an Azure Security Support Engineer at Microsoft. He has previously worked as an independent SIEM Solutions Consultant, as well as Systems Security Specialist at Deloitte Canada. He has completed a post-graduate diploma in Network and Systems Security Analysis from George Brown College. Jason is looking to complete his Master's of Science in Cybersecurity in May of 2022.

Stephen Neville is a General Manager at a golf course in South Carolina. He finished his undergrad at Northeastern University with a degree in Information Technology. Once completed, he turned his focus on a M.S. in Cybersecurity that will be completed in 2022.

Sheetal Singh is currently a full-time graduate student and teaching assistant pursuing a M.S. in Cybersecurity at Northeastern University. In her free time, Sheetal works to mentor women pursuing the tech industry in the Boston area through hack-a-tons and organizations. She has experience working full-time at companies such as iSpecimen and HubSpot as a Software Engineer on the backend and frontend. Sheetal holds a B.S. in Computer Science and Cyber Operations from Northeastern University, as well as an A.S. in Science and Mathematics from Oakton Community College.

Brianna Weinstein is a student at Northeastern University while she works full-time for PricewaterhouseCoopers on the Cyber Penetration Testing Team. She earned a B.S in Cybersecurity program in May 2021 and she will graduate with a M.S. in Cybersecurity in May 2022. She is an alumnus of Northeastern University's Collegiate Cyber Defense Competition Team and participated in a number of blue team competitions during her undergraduate education. In her free time, Brianna enjoys walking her dog and listening to podcasts.