NATIONAL
UNIVERSITY

Using Devops Tools to Deploy Cybersecurity Labs in Cloud Computing Environments

Christopher Simpson
Director, National University Center for Cybersecurity

OVERVIEW

- Hands-on cybersecurity labs are an excellent way to teach cybersecurity and for students to demonstrate knowledge. Due to the use of proprietary software and other factors like significant hardware requirements and large file sizes, it can be difficult to replicate these lab environments. The emergence of low cost cloud computing resources and the automated deployment of infrastructure using devops tools make it easier to share and deploy lab resources.

Agenda

- Overview
- Description of Devops
- Tools
- Process
- Demo

Background

- Hands on labs are a critical component of any cybersecurity program and a CAE requirement
- Several ways to deliver lab content
  - Develop and deploy labs on internal or outsourced infrastructure
  - Utilize labs from external lab providers
  - Utilize free grant resourced labs
  - Use free and open source labs

Background

- Presentation derived from AMCIS 2019 paper.
  - "Automated Deployment of Cybersecurity Labs in Cloud Computing Environments"
    - Christopher Simpson, Dr. Omar El-Gayar, and Dr. Dave Bishop

Cloud Based Labs

- On demand self service
- Customization
- Examples
  - Edurange

What is Devops?

- “DevOps is a development methodology aimed at bridging the gap between Development (Dev) and Operations, emphasizing communication and collaboration, continuous integration, quality assurance and delivery with automated deployment utilizing a set of development practices.” (Jabbari, Ali, Petersen, & Tanveer, 2016)
- Can be applied to the deployment of IT infrastructure (Artac et al. 2017)

Infrastructure as Code (IaC)

- "The management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code."
  - https://docs.microsoft.com/en-us/azure/devops/learn/what-is-infrastructure-as-code

Devops Tools

- Orchestration Tools
  - Terraform, Cloud Formation
- Configuration Management
  - Chef, Puppet, SALT, Ansible
- Continuous Integration
  - Jenkins, Travis
- Version Control
  - Git

Three Examples of Cloud Based Labs

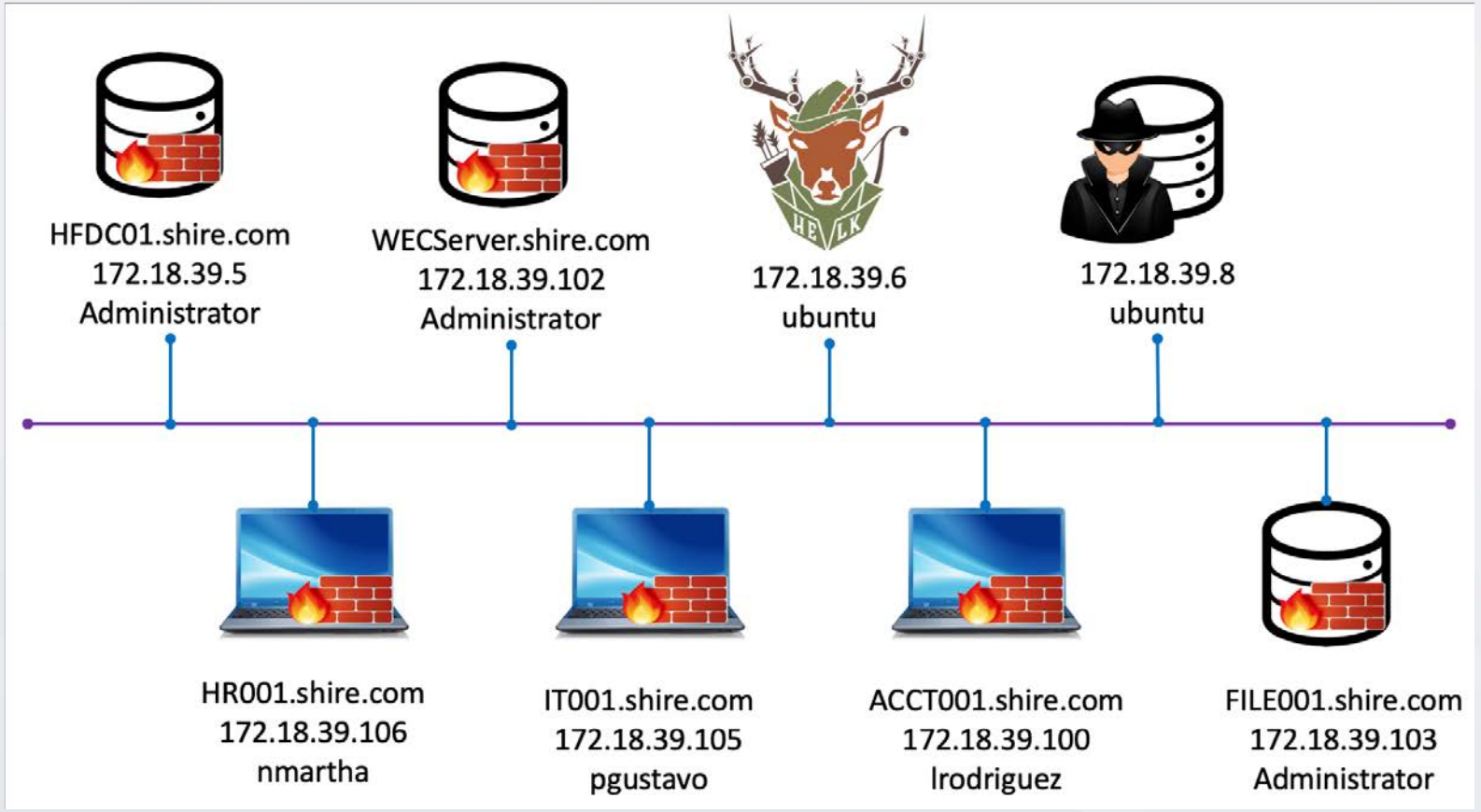
- Mordor Gates
- Detection Lab
- CyberRange

Mordor

- "The Mordor project provides pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON) files for easy consumption”
- Pre-built security events
- Mapped to Mitre ATT&CK Framework
- Several datasets

Mordor Environment

- Designed for Threat Hunting
- Pre-built data collection



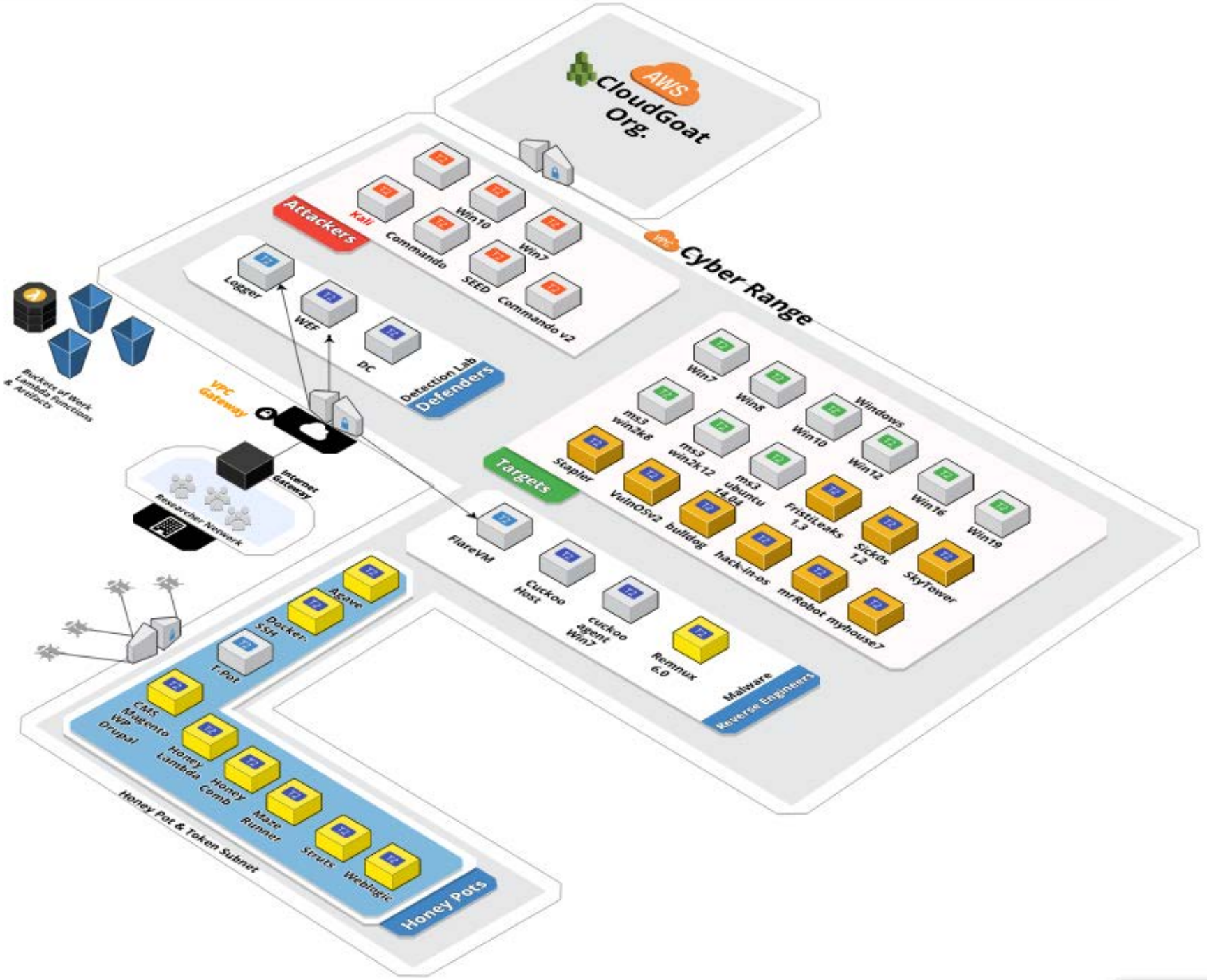
Detection Lab

- Pre-built Windows Domain
- Microsoft Advanced Threat Analytics
- Splunk and pre-built Splunk Forwarders
- Osquery connected to a Fleet server
- Sysmon
- Multiple deployment options
  - VMWARE/ESXi
  - AWS
  - Virtual Box
  - Requires Vagrant

CyberRange

- Pre-built Cyber range
- Attack VM's
- Pre-built target VM's
- Reverse engineering
- Honeypots
- Incorporates detection lab
- Built on AWS
  - Azure in the works

CyberRange



NATIONAL UNIVERSITY

Required Tools

- AWS Command Line Interface
- AWS account
  - AWS Access key
- Terraform
- Git
- Will work in other cloud environments with modifications

Demo Time

- Some familiarity with AWS and AWS CLI

Set Up

- Integrated Development Environment
  - Visual Studio Code
- Version Control System
  - Github
- Infrastructure as Code Tool
  - Terraform
- AWS Account
  - AWS Educate for free credits
- Project sign up (if required)

Terraform

- Install terraform
- Protect your credentials
- Don’t put your credentials in your code

```
1   region = "us-west-1"
2   #profile = "terraform"
3   shared_credentials_file = "~/.aws/credentials"
4   public_key_name = "linux"
5   public_key_path = "~/.ssh/linux.pub"
6   private_key_path = "~/.ssh/linux"
7   ip_whitelist = ["172.251.211.216/32"]
```

Costs

- It’s very easy to spin up dozens of VM’s, remember you pay by the minute
- Set up billing alerts

Demo

Summary and Future Work

- Devops tools can be used to deploy labs into cloud computing environments
- Map open source labs to KU's and NICE Framework
- Map open source labs to classes

QUESTIONS ?

Email: csimpson@nu.edu

References

- Detection Lab
  - https://github.com/clong/DetectionLab
- CyberRange
  - https://medium.com/aws-cyber-range
  - https://github.com/secdevops-cuse/CyberRange
- Project Mordor
  - https://github.com/hunters-forge/mordor
- Terraform
  - https://www.terraform.io