Introduction

DetectionLab

- @jaw33sh
- Started as CTF player
- Multiple CTF winner
- Cars and hacking

Agenda

- What is DetectionLab and requirements
- Dev-Ops in a nutshell
- Use cases.
- Demos
- Lessons learned while testing

- Collection of scripts
- Windows active directory with logging and endpoint security
- Best practices
- Lab
  - *DC*
  - *WEF*
  - *Win10*
  - *logger*

Tools within

- Microsoft Advanced Threat Analytics
- Splunk forwarders
- A custom Windows auditing configuration
- Palantir's Windows Event Forwarding
- Powershell transcript logging is enabled
- osquery
- Sysmon SwiftOnSecurity’s open-sourced configuration

Tools within

- Splunk Enterprise
- Kolide osquery Manager
- Bro
- Suricata
- autostart items are logged to Windows Event Logs
- SMBv1 Auditing is enabled

Requirement

- **55+** GB disk space
- **16+** GB RAM
- Packer 1.3.2 or newer
- Vagrant 2.2.2 or newer
- VirtualBox, VMware or clouds

Kali

DetectionLab

Dev-ops crash course

Vagrant

- Simplify deployment (no more it works on my machine)
- Deploy to hypervisors/cloud

Packer

- Create identical machine images for multiple platforms from single conf file.

- Building and provision (gold)-images

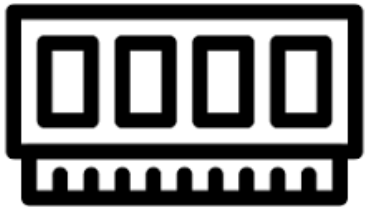
Terraform

- Deploy on the clouds
- Building/provisioning scripts

Pain and sufferance

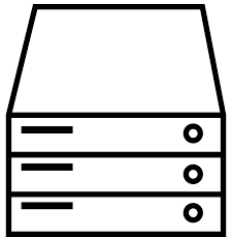
HashiCorp Packer

1.4 vs 1.3.5



RAM

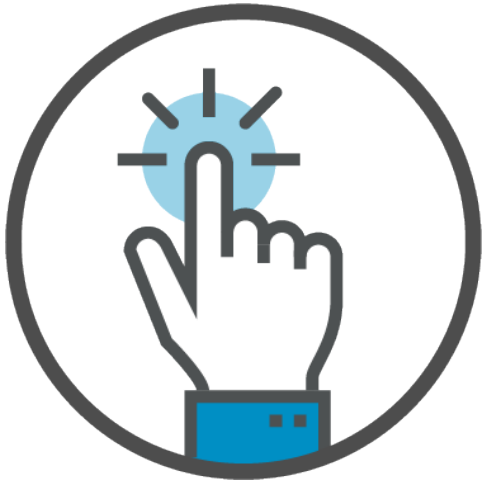
Errors



Disk space

Use cases

- DFIR pros who want to see attack fingerprints.
- Bug bounty hunter who wants to quickly test on AD.
- Red team member who want to check his forensics artifacts.
- Learning security tooling automation.
- Staging environment to see security tooling effects.



DEMO

Take Away

- Save time by automation to create AD environment.
- Highly customizable.
- DL is not hardened!.
- Beneficial for Red, Blue and purple teams.
- FAST.

Resources and Q&A

https://github.com/clong/DetectionLab

https://dev.to/azure/presentation-tips-for-technical-talks-1fni