



# Building a Home Hacking Lab for Testing and Fun

# \$ whoami

- ▶ Jimmy Lloyd
- ▶ Principal Security Analyst/Penetration Tester at Bank of New York Mellon
- ▶ Father of 3
- ▶ DevSecOps and Security Automation enthusiast
- ▶ @jacoll on twitter
- ▶ <https://github.com/jaconll12>

# Cyber Security PSA

- ▶ Humility goes a long way
  - ▶ Imposter Syndrome is a real thing
  - ▶ Don't let arrogance or feeling inadequate consume you
  - ▶ Everyone has some value to add no matter how novice you are.
- 
- ▶ “A true genius admits that he/she knows nothing.” — **Albert Einstein**
  - ▶ “There is nothing noble in being superior to your fellow man; true nobility is being superior to your former self.” — **Ernest Hemingway**

# Getting started in IT/Cyber Security

- ▶ What is the best way to learn anything in IT?
  - ▶ Play – Break – Fix – Try again
- ▶ The same thought process works for IT Security



# Why a home lab is important

- ▶ So you want to get started in learning, what is your first step
  - ▶ 1. Download and install Kali Linux
  - .....
  - ▶ 2. Now what
    - ▶ Hack your neighbors?
    - ▶ Hack your work systems?
    - ▶ Search Shodan for vulnerable systems to attack?

**2 days ago I named my WiFi to "Hack it if you can" and..**



**yesterday it was changed to  
"Challenge accepted"**

# Cyber Security Related Laws

- ▶ 1974 Privacy Act
- ▶ Electronic Communications Privacy Act (ECPA) 1986
- ▶ Computer Fraud And Abuse Act (CFAA)
- ▶ 2011 Cyber Intelligence Sharing And Protection Act (CISPA)
- ▶ 2012 Children's Online Privacy Protection Act (COPPA)
- ▶ And the list goes on ....

0	1	2	3	4	5	6	7	8	9	10	11
A person commits a "computer crime" when he or she:											
1. accesses a computer system without authorization;											
2. accesses or uses a computer system to obtain unauthorized computer services (including computer access, data processing, and data storage);											
3. intentionally or recklessly disrupts, degrades, or causes disruption or degradation of computer services or denies or causes denial of computer services to an authorized user; or											
4. intentionally or recklessly tampers with, takes, transfers, conceals, alters, or damages any equipment used in a computer system.											
It is also a computer crime to misuse computer system data. A person commits this crime by:											
1. accessing a computer system to use, disclose, or copy data residing in, communicated by, or produced by a computer system;											
2. intentionally or recklessly and without authorization (a) tampering with, damaging, or taking data intended for use by a computer system or (b) intercepting or adding to data residing within a computer system;											
3. knowingly receiving or retaining data obtained through misuse of computer system information; or											
4. using or disclosing data he or she knows or believes was obtained through misuse of computer system information (CGS § 53a-251).											

<https://www.cga.ct.gov/2012/rpt/2012-R-0254.htm>

**Table 1: Degrees of Computer Crime and the Requirements for Each Penalty (CGS § 53a-252 et seq.)**

Degree of Computer Crime	Amount of Damage or Harm Required	Penalty
1 <sup>st</sup> degree	Damage to or the value of the property or computer services is over \$10,000	B felony (up to 20 years in prison, a fine of up to \$15,000, or both)
2 <sup>nd</sup> degree	Damage to or the value of the property or computer services is over \$5,000	C felony (up to 10 years in prison, a fine of up to \$10,000, or both)
3 <sup>rd</sup> degree	<ul style="list-style-type: none"> <li>• Damage to or the value of the property or computer services is over \$1,000</li> <li>• Reckless conduct that creates a risk of serious physical injury to another person</li> </ul>	D felony (up to five years in prison, a fine of up to \$5,000, or both)
4 <sup>th</sup> degree	Damage to or the value of the property or computer services is over \$500	A misdemeanor (up to one year in prison, a fine of up to \$2,000, or both)
5 <sup>th</sup> degree	Damage to or the value of the property or computer services, if any, is \$500 or less	B misdemeanor (up to six months in prison, a fine of up to \$1,000, or both)

# Cyber Crime

# “Ethical Hacking”

“... ethical hacking is to evaluate the security of and identify vulnerabilities in systems, networks or system infrastructure. It includes finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible.”



<https://searchsecurity.techtarget.com/definition/ethical-hacker>

# Why a home hacking lab is fun



- ▶ Virtual Playground
- ▶ Hands on approach to learning
- ▶ Hacking is a lot of fun

# Additional Benefits of a Home Lab



Mimic real-world environments



Best way to learn about a technology is to build it yourself



Test new toolsets

# 100% Online Options

## ▶ HacktheBox

- ▶ Has a paid and a free option
- ▶ VIP is \$10/moth or \$100/year
- ▶ <https://www.hackthebox.eu/home/machines>

## ▶ Attack Defense

- ▶ Has a cost associated but the labs are very comprehensive
- ▶ Normally \$69/month currently \$39/month
- ▶ <https://www.attackdefense.com>

## ▶ Other Options

- ▶ <https://www.hackthissite.org>
- ▶ <https://www.enigmagroup.org>

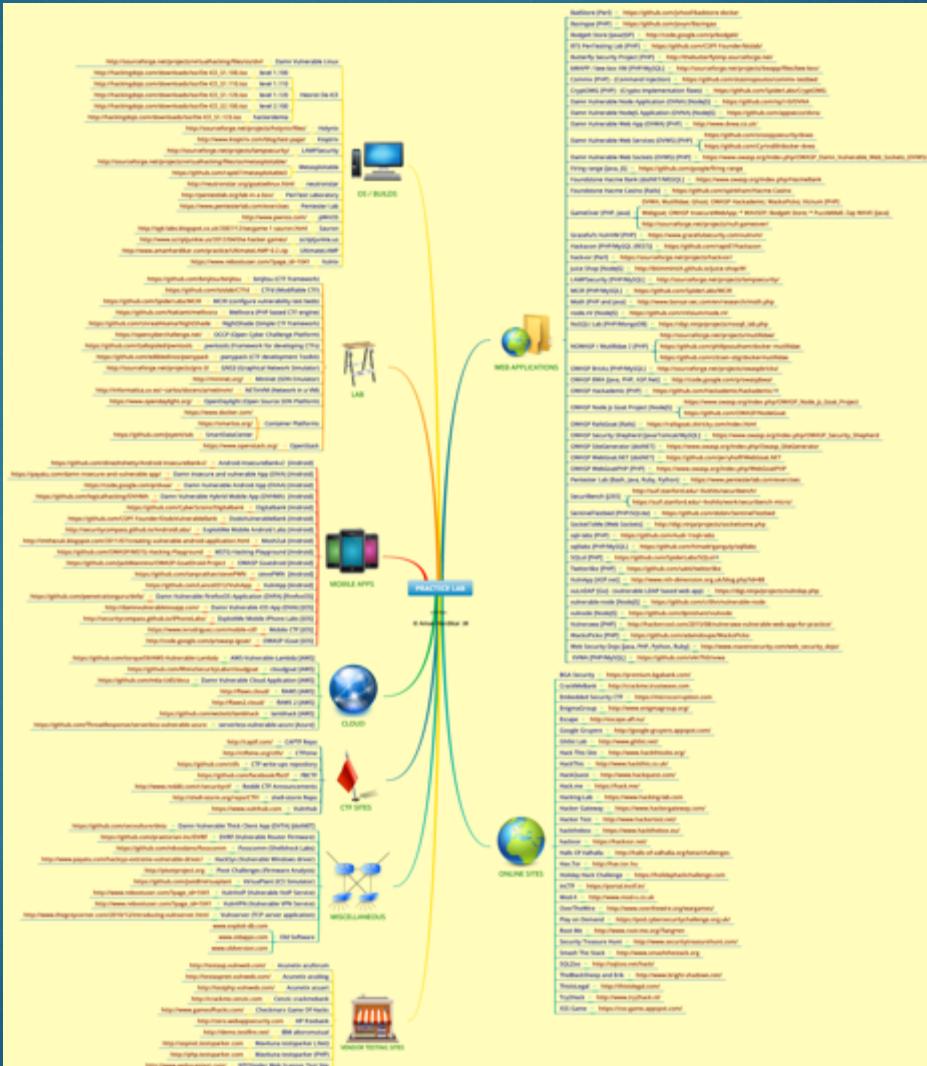
The image displays two screenshots of online hacking platforms. The top screenshot is from HackTheBox, showing the 'Machine Lab' section with information about VIP machines and a call-to-action button. The bottom screenshot is from Attack Defense, showing the 'ATTACK DEFENSE' dashboard with statistics like 'Total Labs' (1202), 'Ongoing Labs' (0), and 'New this Month' (41). Both sites feature navigation menus on the left and lists of available labs or machines on the right.

# Now let's build your home hacking lab...



- ▶ Plan your focus
- ▶ Design a plan
- ▶ Segment your lab network
- ▶ Install/Purchase the tools you need
- ▶ Research ...

# Information OVERLOAD



<https://www.amanhardikar.com/mindmaps/Practice.html>

# Different options for your lab

- ▶ Bare Metal
- ▶ Cloud
- ▶ Virtualization



# Cloud vs Physical

- ▶ Cloud computing is on-demand computing services
- ▶ Cloud Options
  - ▶ Amazon Web Services (AWS)
  - ▶ Google Cloud Services (GCS)
  - ▶ Microsoft Azure
  - ▶ VPS Services
- ▶ Physical (In House)



# Pros/Cons of Cloud

- ▶ Pros
  - ▶ Speed
  - ▶ Agility
  - ▶ Cost
- ▶ Cons
  - ▶ Cost
  - ▶ Networking
  - ▶ Traffic Flow

Microsoft Windows Server 2019 Base				
Microsoft		Pricing Details		
		Hourly Fees		
Instance Type	Software	EC2	Total	
t1.micro	\$0.00	\$0.02	\$0.02/hr	
t2.nano	\$0.00	\$0.008	\$0.008/hr	
t2.micro	\$0.00	\$0.016	\$0.016/hr	
t2.small	\$0.00	\$0.032	\$0.032/hr	
t2.medium	\$0.00	\$0.064	\$0.064/hr	
t2.large	\$0.00	\$0.121	\$0.121/hr	
t3a.nano	\$0.00	\$0.009	\$0.009/hr	
t3a.micro	\$0.00	\$0.019	\$0.019/hr	
t3a.small	\$0.00	\$0.037	\$0.037/hr	
t3a.medium	\$0.00	\$0.056	\$0.056/hr	
t3a.large	\$0.00	\$0.103	\$0.103/hr	
t3a.xlarge	\$0.00	\$0.224	\$0.224/hr	
t3a.2xlarge	\$0.00	\$0.448	\$0.448/hr	
t3.nano	\$0.00	\$0.01	\$0.01/hr	
t3.micro	\$0.00	\$0.02	\$0.02/hr	
t3.small	\$0.00	\$0.039	\$0.039/hr	
t3.medium	\$0.00	\$0.06	\$0.06/hr	
t3.large	\$0.00	\$0.144	\$0.144/hr	

# Cloud Demo



# Amazon Web Services

The screenshot shows the AWS Marketplace search results for "Windows Server". The search bar at the top contains "Windows Server". Below the search bar, there are two tabs: "Categories" and "aws marketplace". The "Categories" tab is selected, showing a sidebar with navigation links like "History", "Console Home", and "Categories". The main content area displays a list of results for "Windows Server (356 results)".

Image	Name	Rating	Description
	<a href="#">Microsoft Windows Server 2019 Base</a>	★★★★★ (2)	Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run compatible Windows-based solutions on AWS' high-performance, reliable, cost-effective, cloud computing platform.
	<a href="#">Microsoft Windows Server 2016 Base</a>	★★★★★ (0)	Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any compatible Windows-based solution on AWS' high-performance, reliable, cost-effective, cloud computing platform. Common...
	<a href="#">Microsoft Windows Server 2012 R2</a>	★★★★★ (0)	Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any compatible Windows-based solution on AWS' high-performance, reliable, cost-effective, cloud computing platform. Common...

At the bottom of the page, there are links for "Migration Mapping Assistant", "Your Saved List", "Partners", "Sell in AWS Marketplace", and "Amazon Web Services Home". The right side of the screen shows a green vertical bar.

# Virtualization



# Full Operating System Virtualization

## Software Options

- ▶ VMWare Workstation/Fusion - \$150-250
  - ▶ VMWare Player - Free
- ▶ Oracle Virtual Box - Free
- ▶ Parallels (MacOS Only) – \$80-100
- ▶ ESXi – Full Hypervisor - Free

# Pros and Cons of VMs

## Pros

- Highly configurable
- Expandable
- Full Operating System level functionality
- Able to limit availability
- Snapshotting

## Cons

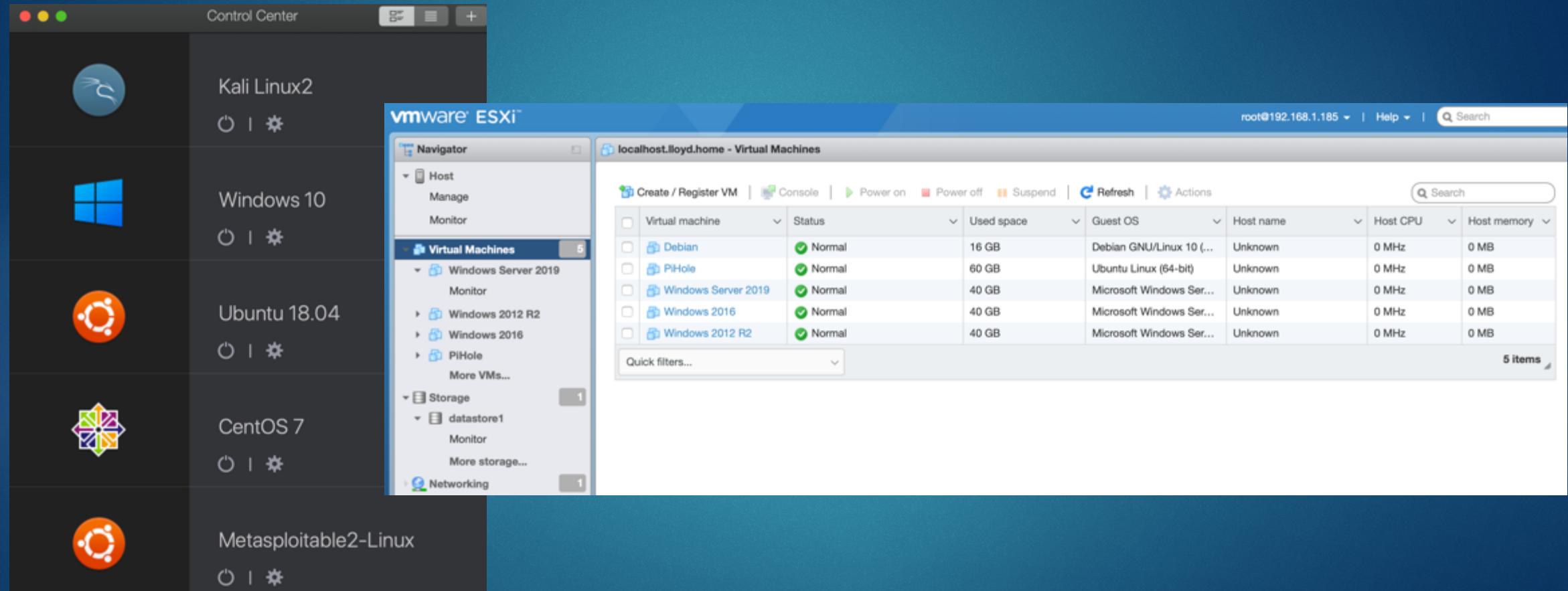
- Resource intensive
- Longer to setup and configure

# Windows 10 Subsystem for Linux

- ▶ Windows Subsystem for Linux, or WSL, is a feature-set in Windows 10 that allows Linux programs to run natively. Its not a true virtual machine, but a virtual environment
- ▶ “Our top requests from the WSL community have been to increase the file system performance, and make more apps work inside of WSL (i.e: introduce better system call compatibility). We have heard your feedback, and are glad to announce that WSL 2 helps solve these issues. WSL 2 is a new version of the architecture that powers the Windows Subsystem for Linux to run ELF64 Linux binaries on Windows. This new architecture changes how these Linux binaries interact with Windows and your computer’s hardware, but still provides the same user experience as in WSL 1 (the current widely available version). Individual Linux distros can be run either as a WSL 1 distro, or as a WSL 2 distro, can be upgraded or downgraded at any time, and you can run WSL 1 and WSL 2 distros side by side. WSL 2 uses an entirely new architecture that uses a real Linux kernel.”

<https://devblogs.microsoft.com/commandline/announcing-wsl-2/>

# My Current Local VM Setup



# Metasploitable

- ▶ Vulnerable Operation System Image
  - ▶ Build by Offensive Security
  - ▶ Offensive Security releases Kali
  - ▶ “A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.”
- 
- ▶ <https://metasploit.help.rapid7.com/docs/metasploitable-2>

# What is Docker?

- ▶ Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all the parts it needs, such as libraries and other dependencies, and ship it all out as one package.
- ▶ Think of Docker as virtualized applications/frameworks



# Pros and Cons of Docker Containers



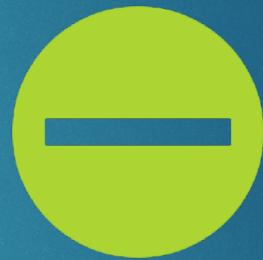
## Pros

Someone has already done all the work for you

Very easy to deploy

Very easy to update

Ability to limit availability



## Cons

Docker images are not very easily customizable

Stability is sometimes an issue

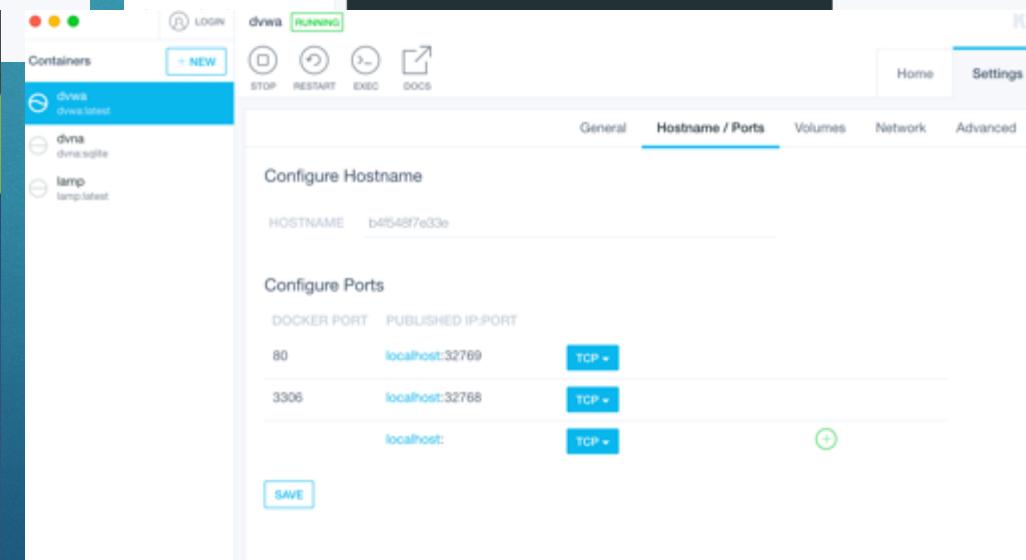
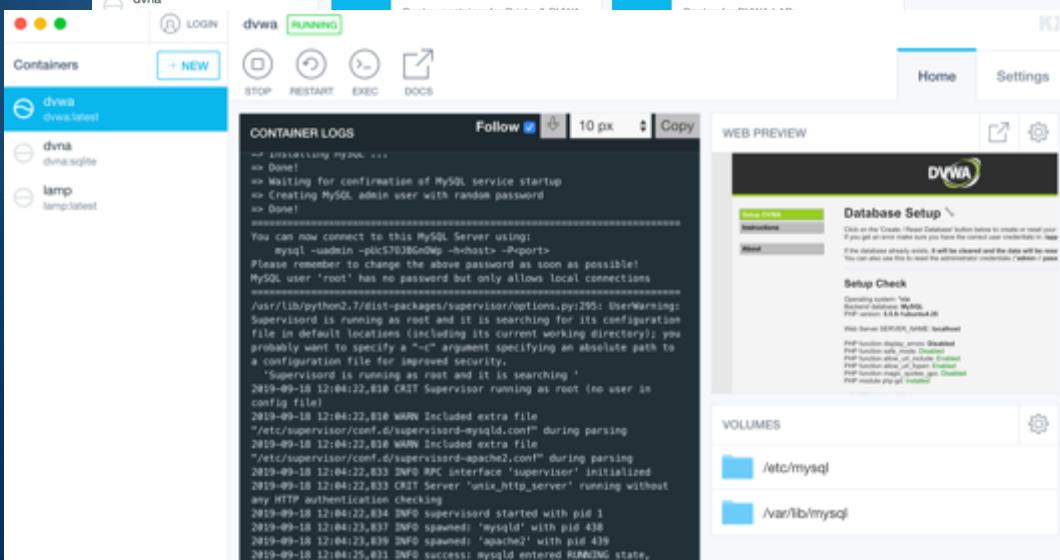
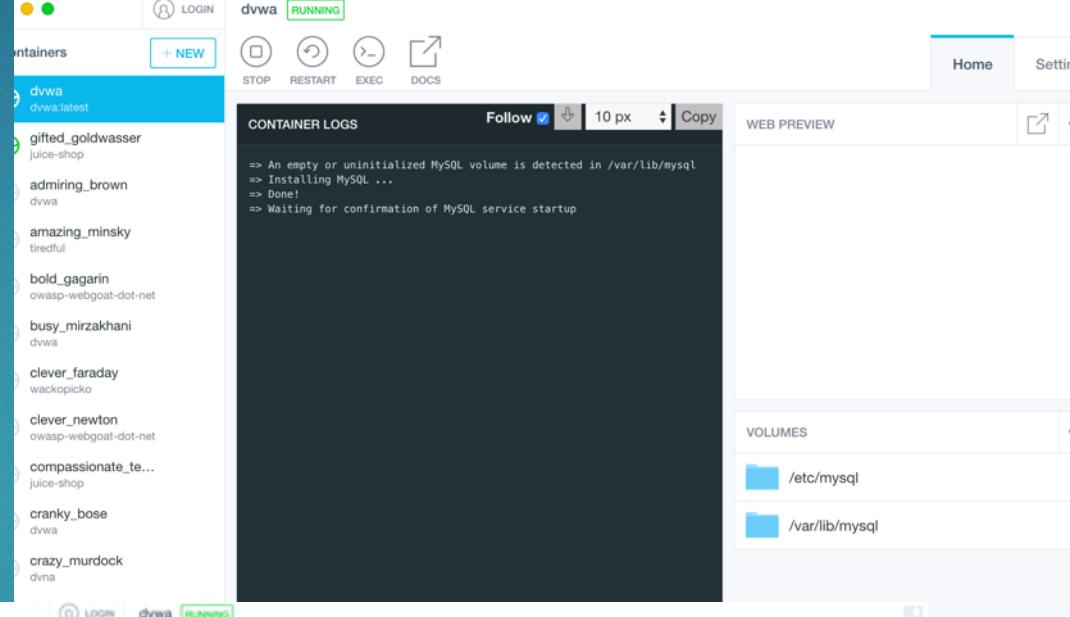
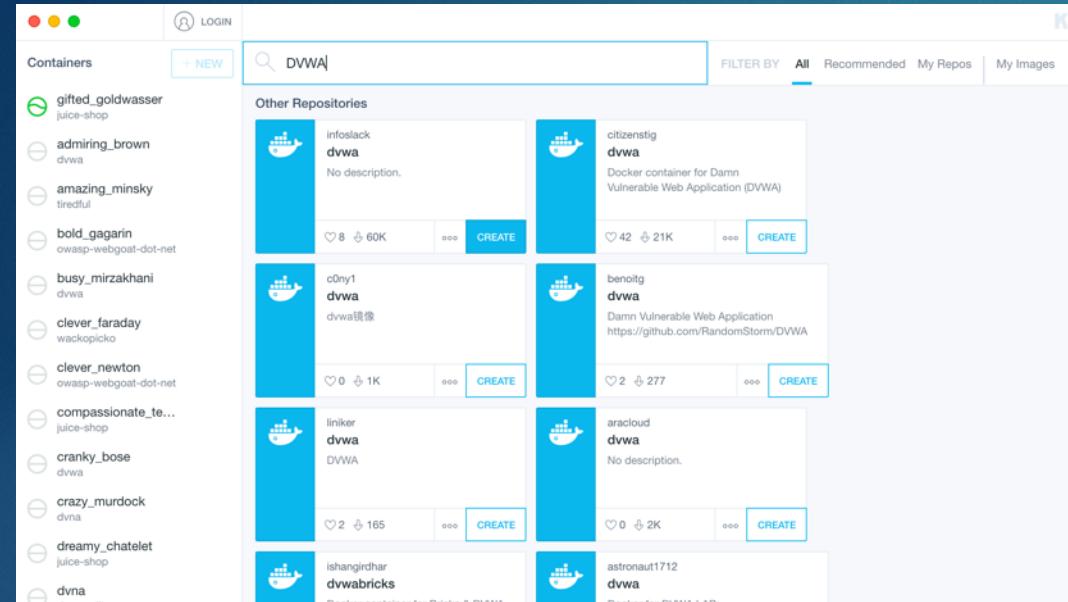
Trust in the source

# Important Docker Commands

- ▶ docker run – Runs a command in a new container.
- ▶ docker start – Starts one or more stopped containers
- ▶ docker stop – Stops one or more running containers
- ▶ docker build – Builds an image from a Dockerfile
- ▶ docker pull – Pulls an image or a repository from a registry
- ▶ docker push – Pushes an image or a repository to a registry
- ▶ docker export – Exports a container's filesystem as a tar archive
- ▶ docker search – Searches the Docker Hub for images
- ▶ docker attach – Attaches to a running container
- ▶ docker commit – Creates a new image from a container's changes

# Kitematic

► A GUI for Docker



# OWASP

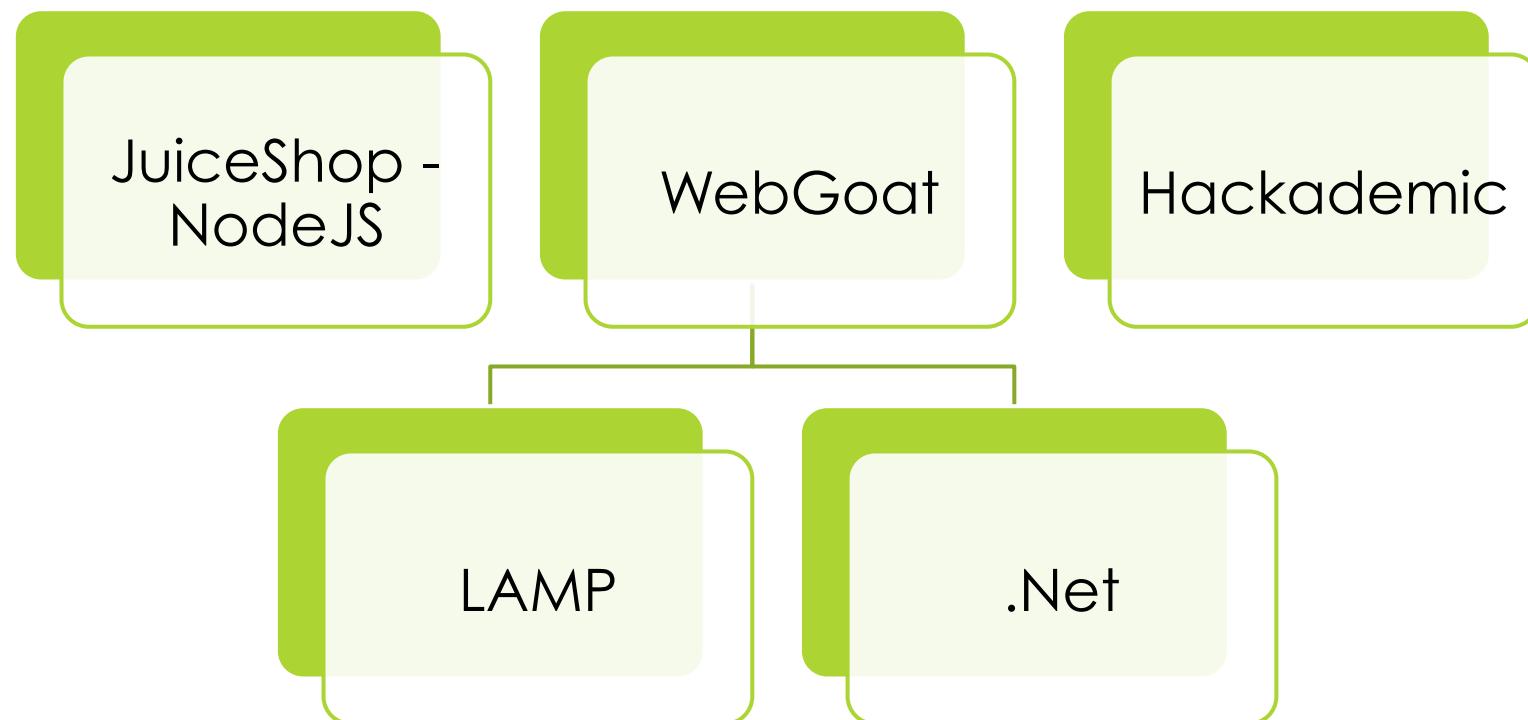
- ▶ “The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions”

[https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)

- ▶ OWASP Top 10

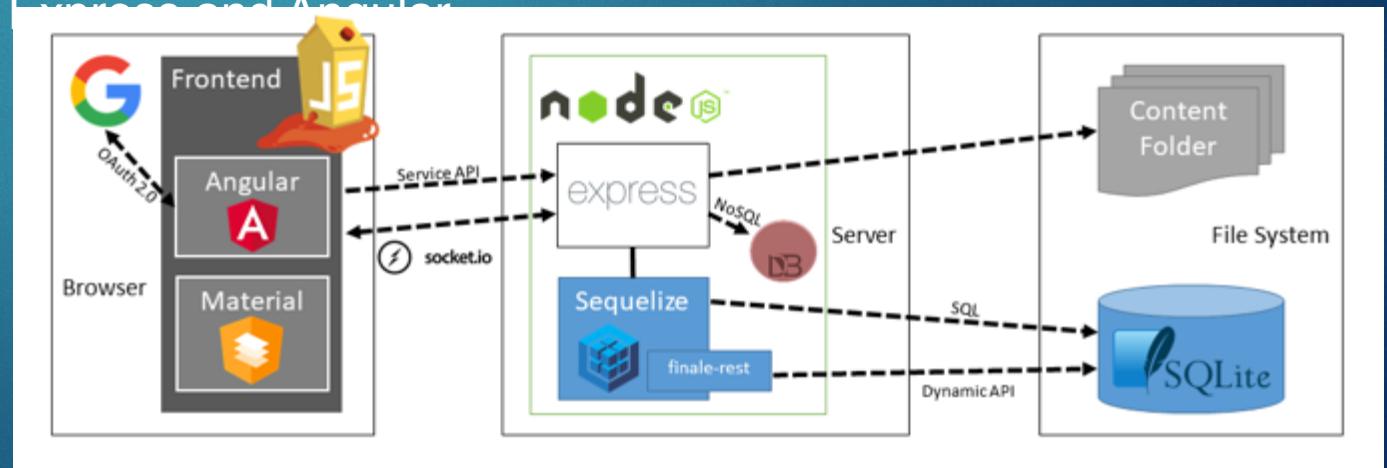
<b>A1:2017 - Injection .....</b>	<a href="#">7</a>
<b>A2:2017 - Broken Authentication .....</b>	<a href="#">8</a>
<b>A3:2017 - Sensitive Data Exposure .....</b>	<a href="#">9</a>
<b>A4:2017 - XML External Entities (XXE) .....</b>	<a href="#">10</a>
<b>A5:2017 - Broken Access Control .....</b>	<a href="#">11</a>
<b>A6:2017 - Security Misconfiguration .....</b>	<a href="#">12</a>
<b>A7:2017 - Cross-Site Scripting (XSS) .....</b>	<a href="#">13</a>
<b>A8:2017 - Insecure Deserialization .....</b>	<a href="#">14</a>
<b>A9:2017 - Using Components with Known Vulnerabilities .....</b>	<a href="#">15</a>
<b>A10:2017 - Insufficient Logging &amp; Monitoring.....</b>	<a href="#">16</a>

# OWASP Images



# OWASP Juice Shop

- ▶ OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications.
- ▶ Juice Shop is written in Node.js, Express and Angular



# JuiceShop Demo



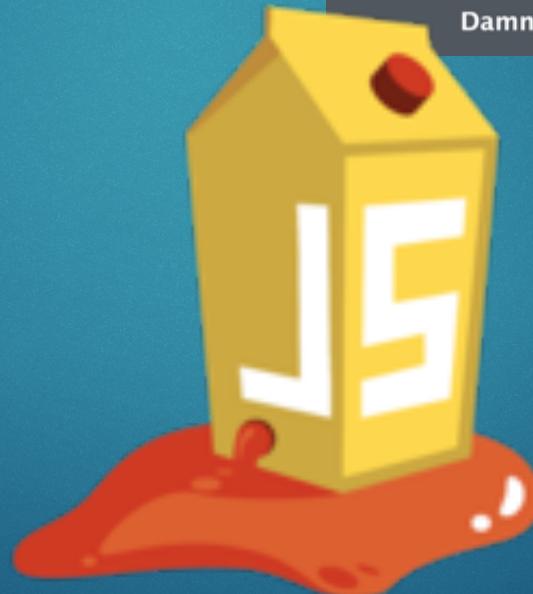
A screenshot of a macOS desktop environment. On the left, a dark-themed application window is open, showing a terminal-like interface with a list of numbers from 1 to 14, each followed by the word "http". The window has tabs for "Dashboard", "Target", "Proxy", "Intruder", "Intercept", "HTTP history", and "WebSoc...". A "Filter: Hidin" dropdown is visible. On the right, a light-themed terminal window titled "jamesclloyd — -bash — 174x38" is open, showing the command "James-MacBook-Pro:~ jamesclloyd\$". The desktop background is dark, and a vertical sidebar on the right shows some file icons.

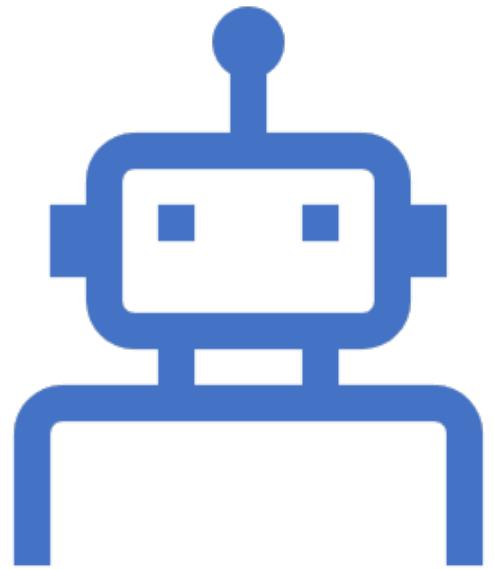
```
#  
1 http  
2 http  
3 http  
4 http  
5 http  
6 http  
7 http  
8 http  
9 http  
10 http  
11 http  
12 http  
13 http  
14 http  
--
```

Messages from Firefox

# Current Docker Setup

- ▶ Damn Vulnerable Web App (DVWA)
- ▶ OWASP JuiceShop
- ▶ OWASP WebGoat.NET
- ▶ Tiredful API
- ▶ WackoPickto





# Lab Demo



# Why This Setup Works for Me

- ▶ I can to test from my host
  - ▶ Home Brew for mac
- ▶ Use of KALI VM
- ▶ Using Docker + Remote/Local VMs allows diversity

# Past interactions of my setup

- ▶ Single Windows 7 on old laptop
- ▶ DISA STIGged Windows Image
- ▶ Any Operating System could get for free
- ▶ Couple Raspberry Pis

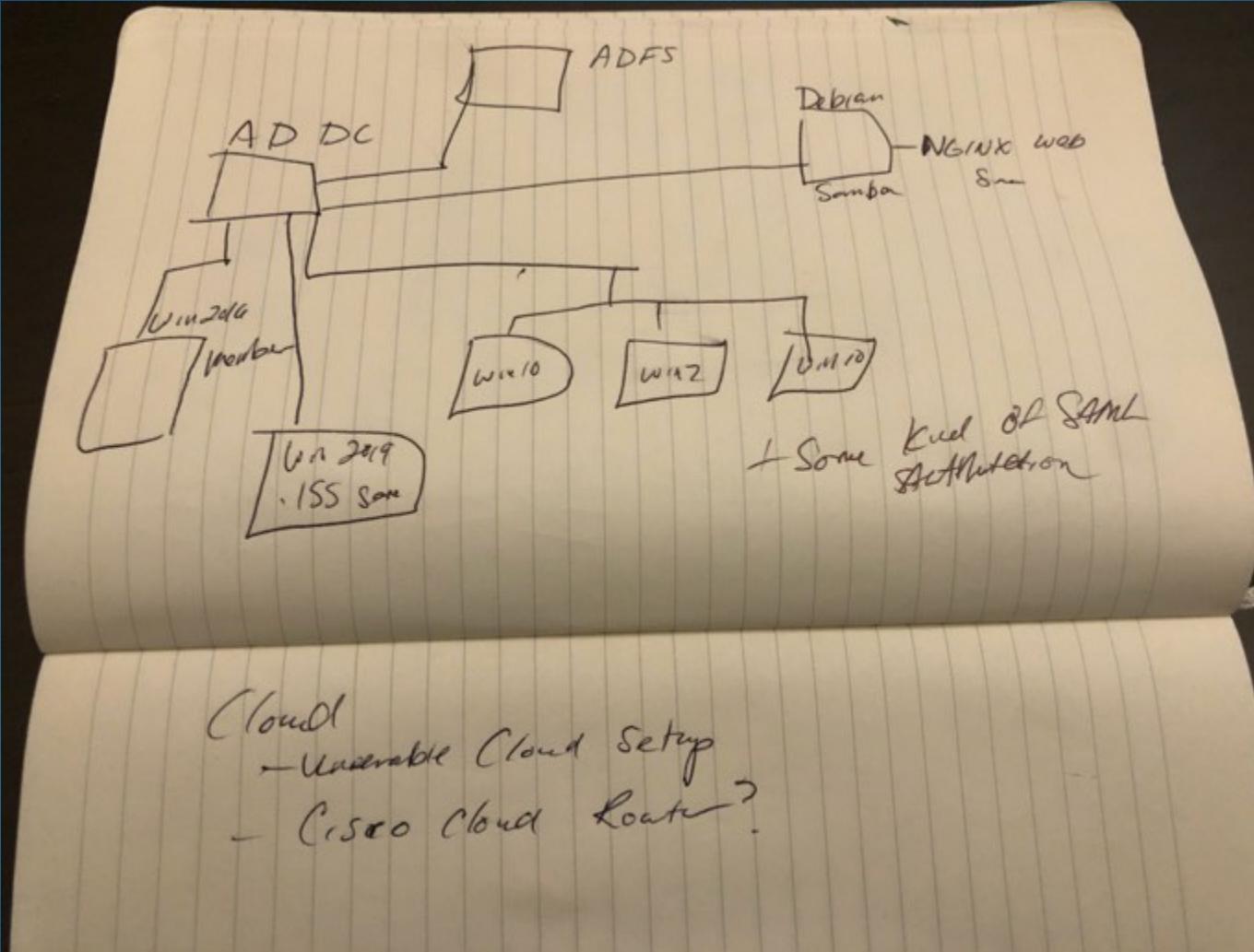
# Past Issues

- ▶ Resources
- ▶ Time
- ▶ Patience

# Future Ideas

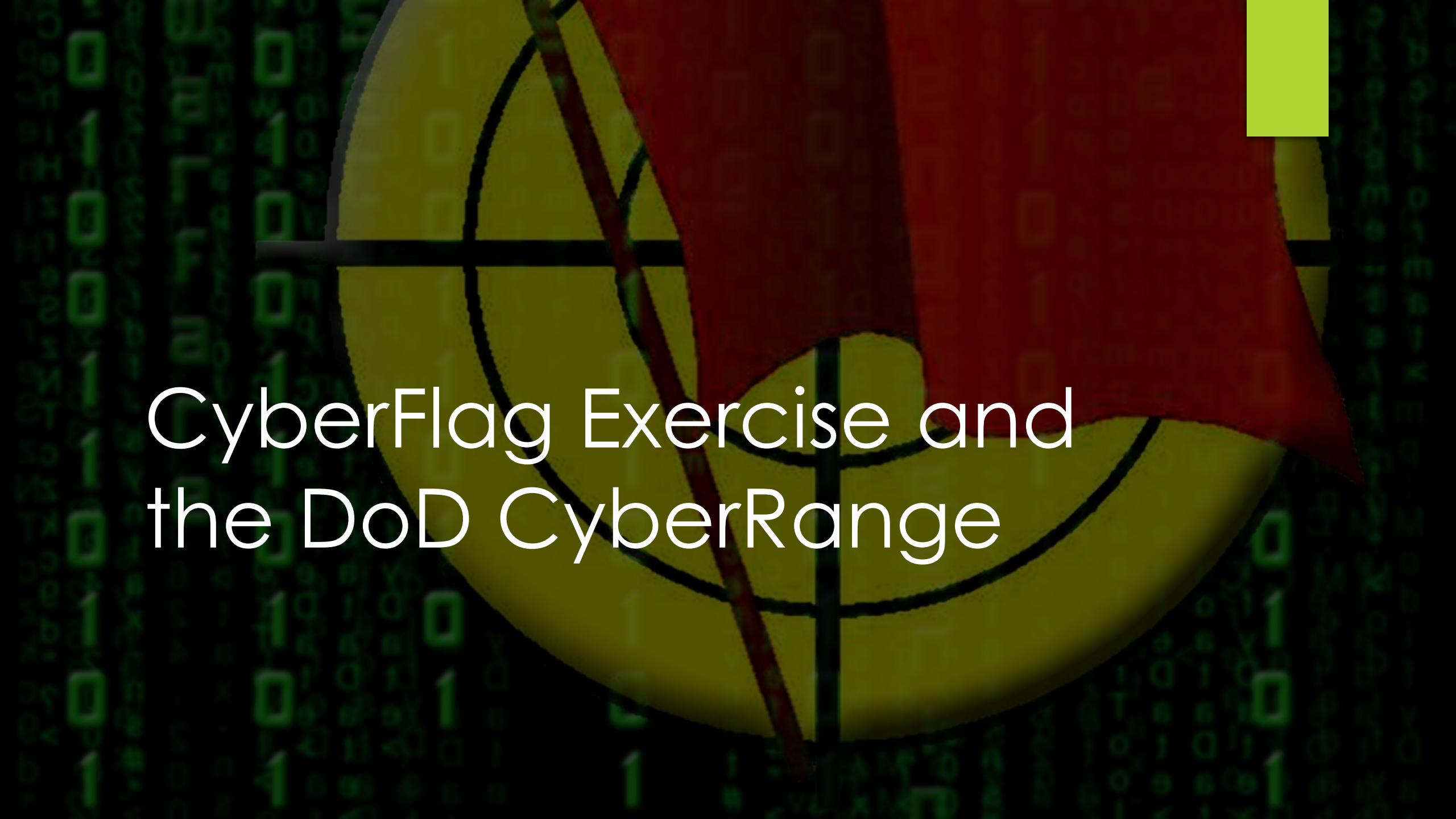
- ▶ ESXi Server hosting most full VM images
- ▶ Build completely “Cyber Range” in my home
- ▶ Build complete Windows Active Directory domain with clients, IIS/.Net web applications, and AD Federated Services
- ▶ Build custom vulnerable web applications (Apache, NGINX)
- ▶ Jenkins CI/CD Pipeline
- ▶ Automate deployment with tools like Puppet and Ansible
- ▶ Web Applications protected by WAF for bypass practice

# Future Logical Diagram



# Real World Testing Scenarios

- ▶ CyAn
  - ▶ Automated web app vulnerability scanner
  - ▶ <https://github.com/jaconll12/CyAn>
  - ▶ Needed a vulnerable web app to test my code
  - ▶ Enter Docker images
- ▶ Exploit development
- ▶ Bug Hunting
- ▶ Training



# CyberFlag Exercise and the DoD CyberRange

# USCyberCommand CyberFlag

- ▶ Department of Defense CyberFlag Exercise
- ▶ Blue Force
- ▶ Red Force (OpFor)
- ▶ White Cell
- ▶ CyberFlag's goal is to mimic real worth threats/APT and train defenders on what to look for

# DoD Cyber Range and DISA MiniFlag

- ▶ DISA "MiniFlag" CyberFlag Prep
- ▶ Full featured VM environment
- ▶ Capable of hosting hundred of guest OS machines
- ▶ Capable of importing almost any toolset
  - ▶ Defender Tools
  - ▶ Red Team Injects
- ▶ My involvement
  - ▶ Build Red Team injects
  - ▶ Developed training plan and exercise flow

# What I Learned from CyberFlag and the CyberRange

- ▶ Having a complete and flexible testing environment is imperative for any profession, especially CyberSec
- ▶ Planning is Key
- ▶ You can create a smaller scale CyberRange at your home ...

# Final Comments

- ▶ You will break EVERYTHING
- ▶ You will make mistakes and screw up ... that's ok that's why you are doing this in a lab
- ▶ You will learn more than you ever could reading books
- ▶ Start Small, then build up....
- ▶ SEGMENT your lab network



# Summary

- ▶ An in-home lab is important for learning and growing
- ▶ Its better than going to jail
- ▶ You do not need a lot of money or experience to get started
- ▶ Cloud, Physical, VM, or Docker
- ▶ Document, document, document
- ▶ Build upon your setup
- ▶ Give back to the community
- ▶ Have some fun
- ▶ Questions/Comments



# References

- ▶ <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016?filetype=ISO>
- ▶ <https://www.offensive-security.com/metasploit-unleashed/requirements/>
- ▶ <https://afourtech.com/guide-docker-commands-examples/>