Code Fellows

Presents

Build Your Own Cyber Range with VirtualBox

By David Lee, Cybersecurity Instructor

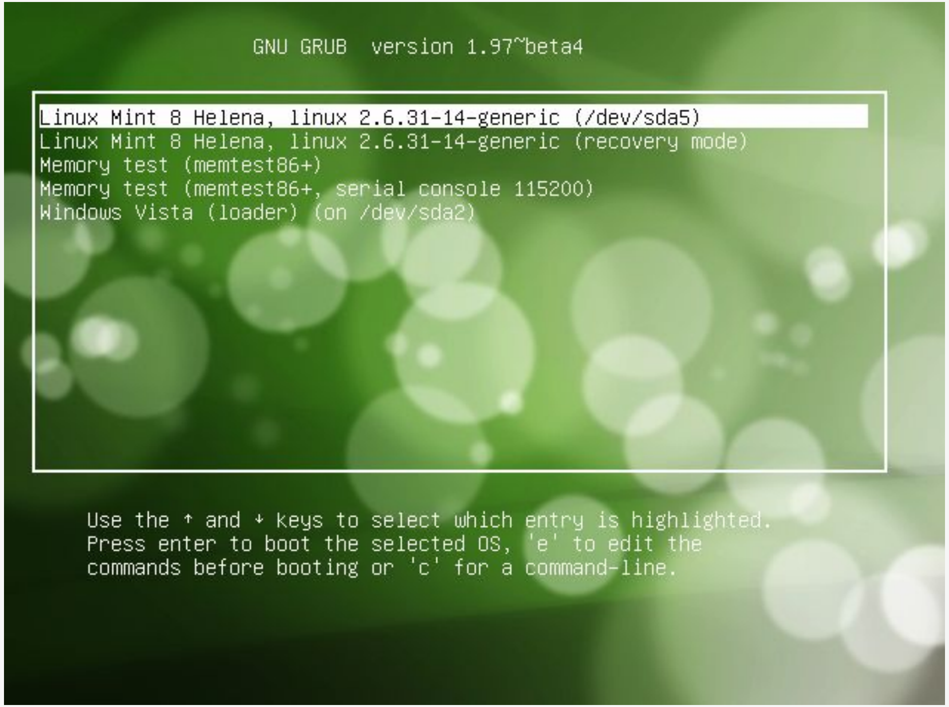
Introduction

- Cyber education volunteer at CSNP
  - Content creator
- Helping career changers start exciting careers in computer operations and cybersecurity at Code Fellows
  - Instructor, curriculum developer
- Background
  - IT, OT, infrastructure, networking, and security
  - M.S. Cybersecurity & Information Assurance
  - CEH, Security+

David Lee
Cybersecurity Instructor, Code Fellows Seattle

Code Fellows

First, a story...



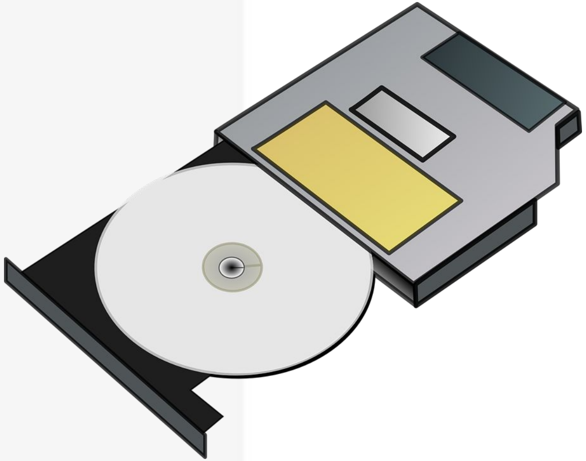
```
GNU GRUB  version 1.97~beta4

Linux Mint 8 Helena, linux 2.6.31-14-generic (/dev/sda5)
Linux Mint 8 Helena, linux 2.6.31-14-generic (recovery mode)
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
Windows Vista (loader) (on /dev/sda2)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting or 'c' for a command-line.
```

Code Fellows

Virtual Machines

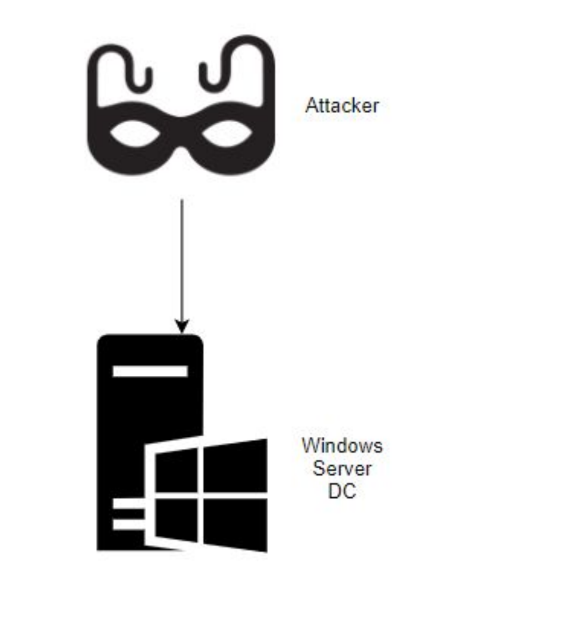
High Level Objectives

- Why am I operating a home lab?
  - Skill development in tooling or scenario
- What should be in my lab?
  - Components necessary to achieve your objective
  - Example: SIEM and IDS for learning defensive SecOps
- How do I source the lab components?
  - ISOs or OVAs of operating systems



What is a Cyber Range?

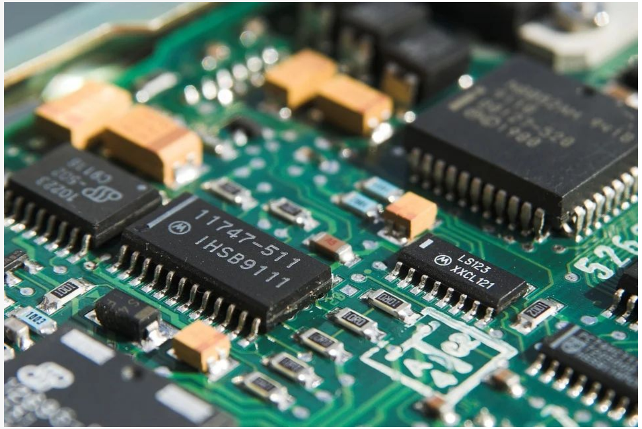
- Controlled virtual environment
- Used for practicing skills in
  - Threat detection
  - Testing attack techniques, scenarios
  - Experimentation
- Can be hosted with:
  - Local physical hardware
  - Cloud IaaS



Code Fellows

Hardware Components

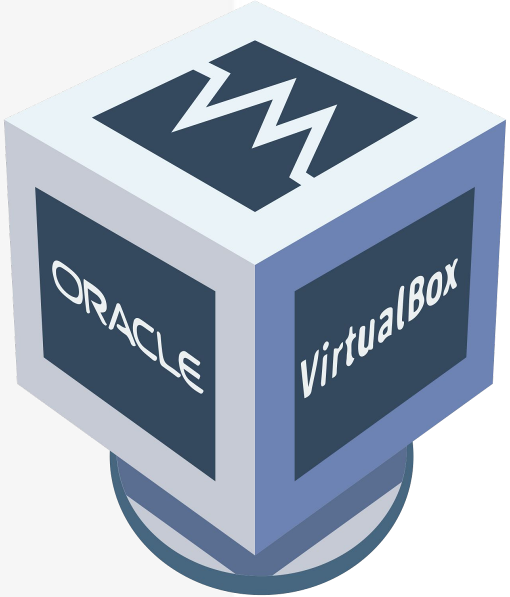
- Virtualization server options
  - A. Dell Precision T3600 ($200)
    - Xeon CPU means more cores
  - B. HP EliteDesk 800 G1 SFF ($2-300)
    - All around solid specs
  - C. Dell PowerEdge R720 ($2-400)
    - Rack-mounted enterprise blade
    - High spec ceiling (RAM, CPU)
    - Loud fans, high power consumption



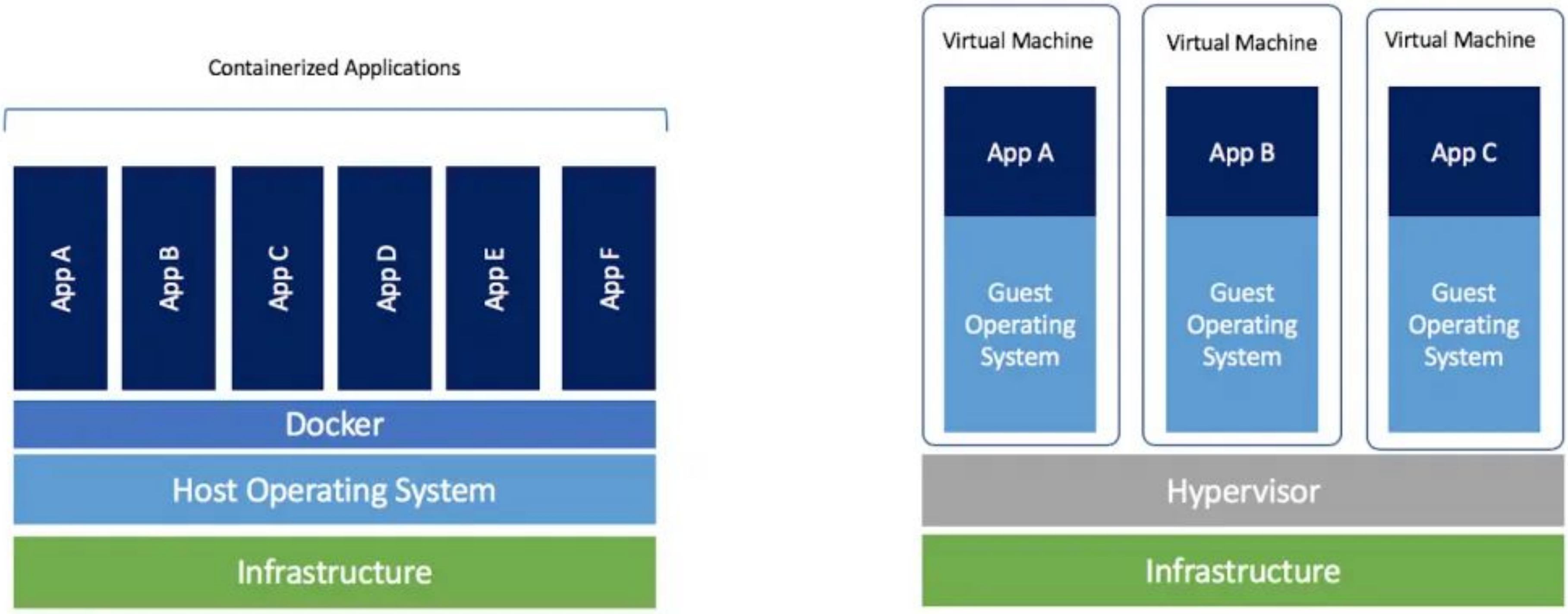
Code Fellows

Why VirtualBox?

- Free!
  - No pay-as-you-go cloud expenses
- Supported on many popular operating systems (Win 10, Ubuntu Linux, etc.)
- Import/export .ova file type for imaging virtual machines (VMs)
- Decent networking capabilities
  - Acts as a router, including DHCP
  - Supports network isolation



VMs or Containers?



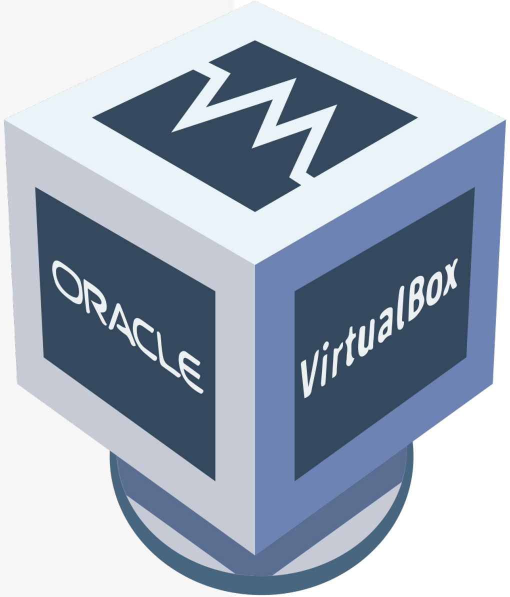
Source: Docker

Code Fellows

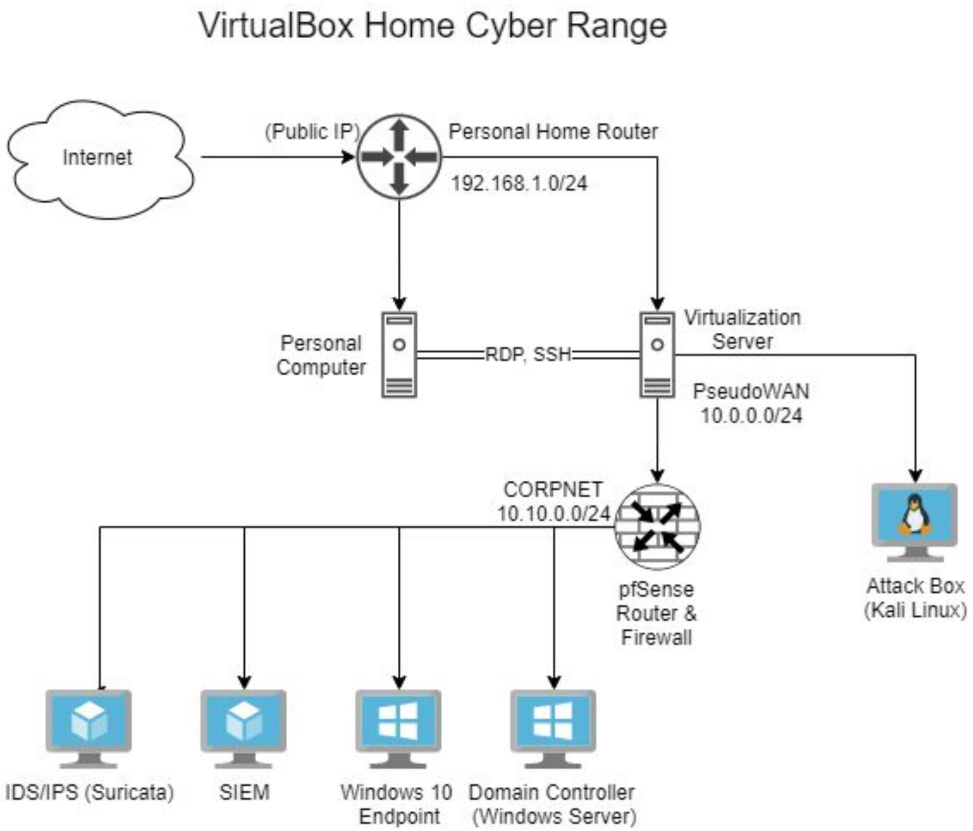
Home Cyber Range

Networking in VirtualBox

- **Bridge Mode**
  - VM is part of the home network
- **NAT**
  - VirtualBox acts as a router with DHCP and performs NAT to put the VM into a subnet
- **NAT Network**
  - Same as NAT but VMs can see each other
- **Host-only**
  - Useful for plugging things in to a pfSense interface

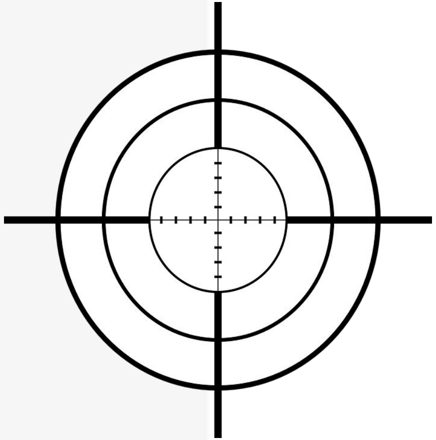


The Network


VirtualBox Home Cyber Range
Internet
(Public IP)
Personal Home Router
192.168.1.0/24
Personal Computer
RDP, SSH
Virtualization Server
PseudoWAN
10.0.0.0/24
CORPNET
10.10.0.0/24
pfSense Router & Firewall
Attack Box (Kali Linux)
IDS/IPS (Suricata)
SIEM
Windows 10 Endpoint
Domain Controller (Windows Server)

The Targets

- PfSense Firewall/Router
  - Traditionally, network perimeter device
- Windows Server DC
  - Primary objective
- Windows 10 endpoint
- SIEM
- IDS/IPS



Networking

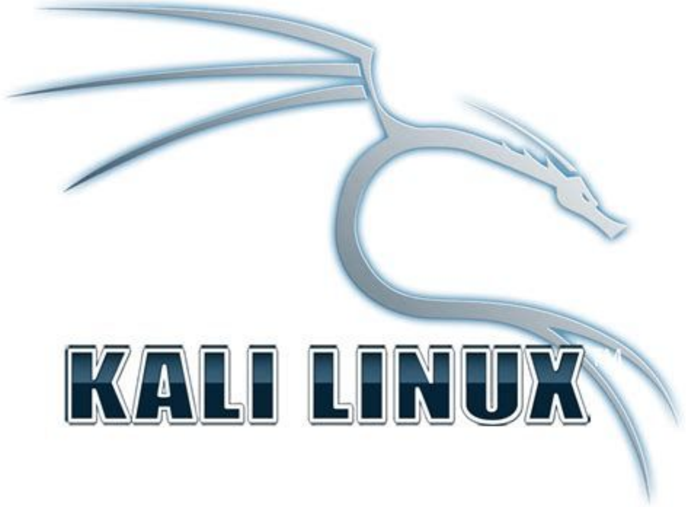
PfSense

- Free open source firewall/router software by NetGate
- Firewall functionality optional
- Extensible using free packages
  - RADIUS captive portal w/ AD
  - IDS/IPS
- Simulate a network perimeter in VirtualBox
- Supports traffic mirroring with span ports

pfsense®

Attacker Box

- Free, open-source Debian distribution
- Preloaded with pentester packages
  - Convenient “toolkit”
- Offensive or intelligence gathering operations



Targets

Windows Server

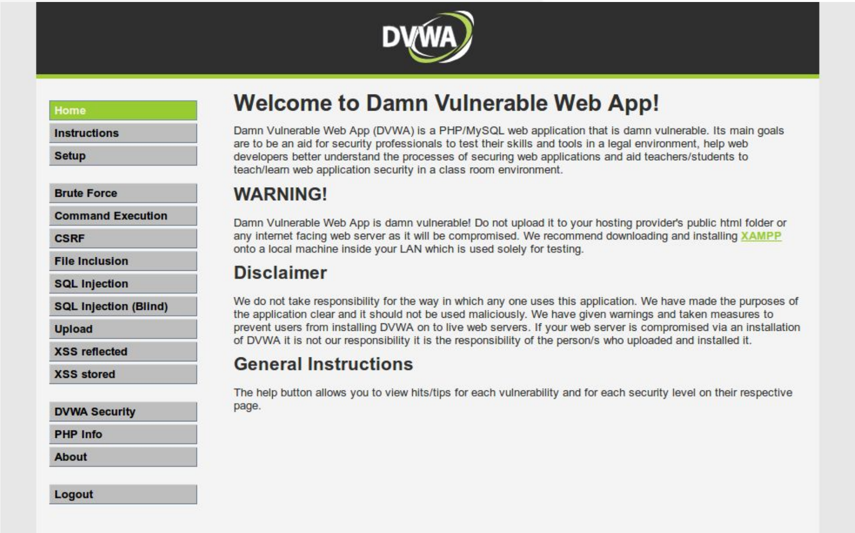
- Usefulness as a target
  - Simulate enterprise architecture
  - Domain Controller (DC)
  - Attractive attack target
  - Privilege escalation attacks and lateral movement, e.g. Mimikatz
- Evaluation editions available free of charge

Splunk SIEM

- Log ingestion from multiple sources
- Query Splunk for important data
- Automate alerts and responses to events
- SPL query language

DVWA for AppSec

- For web application pentesting
  - Includes vulnerabilities
  - Downloadable as OVA



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Demo

Code Fellows

Q&A

Build Your Own Cyber Range with VirtualBox