Building Home Labs

For Fun & Career Development

Michael Miller

Agenda

- Introduction
- What are Home Labs & Why Should You Care
- How Do You Build a Home Lab
- Considerations When Building
- Now What To Do With It
- Security Labs
- Q&A and Resources

$>Whoami

- Cybersecurity Platform Engineering Manager at Cardinal Health
- IT/Cybersecurity for 11+ years in a variety of industries
- Worked with companies ranging in size from <$1M to >$100B
- BS Cybersecurity & Information Assurance from WGU
  AAB Network Administration & Computer Programming from NSCC
- CCSP, SSCP, CEH, ECES, CySA+, Security+, Network+, A+, Project+, CCFA, CCFR
- Participate in InfraGard, ISSA, (ISC)2, Advisory Board for NSCC, CAMO at NSCC, Adjunct Teacher at NSCC
- I enjoy spending time with family, grilling/smoking, tinkering with my home lab, and traveling

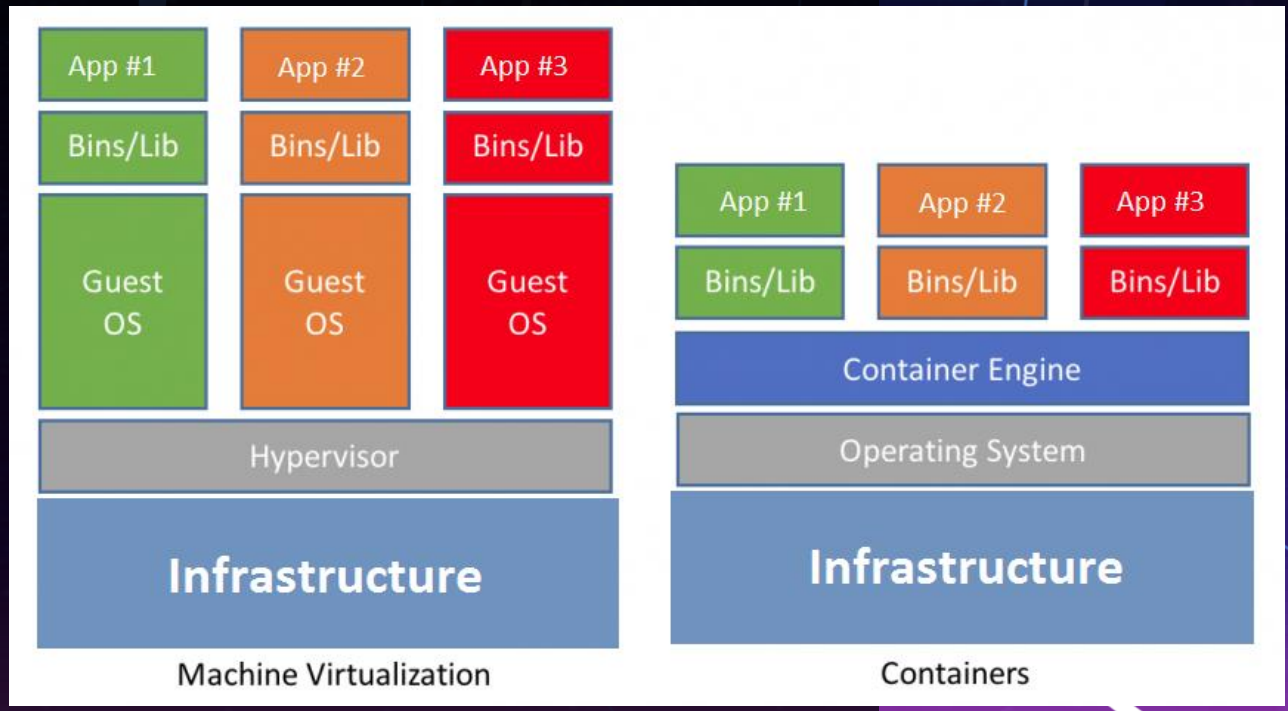
What & Why

- What
  - Home labs are basically a test environment at home
  - Can be containers (Docker/LXC)
  - VM (Virtual Box/VMware/Parallels)
  - Full enterprise network with switching, VLANs, hypervisors, NAS, etc
- Why
  - **Why not, it's fun!**
  - Learn new concepts or technologies (networking, system administration, programming, pen testing, forensics, etc)
  - Test out ideas or changes without effecting a production environment
  - Implement services at home (e.g. PiHole, Plex, NextCloud, GitLab, Network monitoring, Security Onion, Syncthing, Wiki, etc)
  - **Resume/skills building**

How - Containerization

Containerization

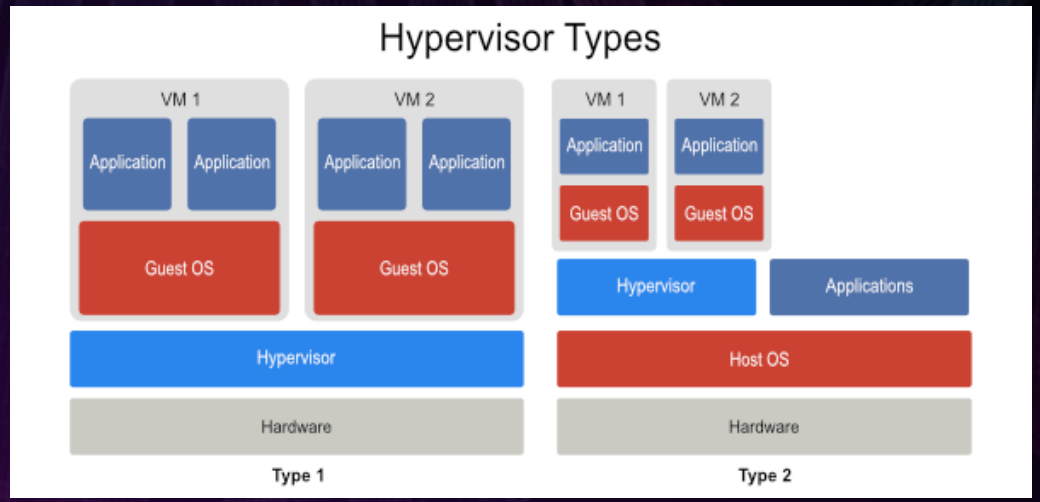
- BSD Jails
- Docker
- Containerd
- LXC/LXD
- OpenVZ
- Kubernetes



How - Virtualization

Type 2 - Hosted

- VMware Workstation/Fusion
- VirtualBox
- Parallels (Mac)
- Hyper-V
- WSL



Type 1 - Bare-Metal

- ProxMox VE
- VMware ESX
- Hyper-V
- Xen

How - Virtualization

Network Virtualization/Simulation

- GNS3
- EVE-NG
- Cisco Packet Tracer
- Cisco VIRL

How - Hardware

- Servers
  - Dedicated or Type 1 Hypervisors
  - Old Computers/Laptops or Refurbished/Auctioned Systems
  - Single Board Computers (Raspberry Pi)
- Storage
  - Appliances – Synology, QNAP
  - Dedicated – FreeNAS Core/SCALE, UnRAID
  - Old Computers & HDDs or Refurbished/Auctioned Systems
- Network Gear
  - MikroTik
  - Ubiquiti
  - Refurbished/Auctioned Systems
  - Firewalls – pfSense, OPNSense, Untangle

How - Cloud

- Azure
- GCP
- AWS
- VPS
  - Digital Ocean
  - Linode

Considerations

- Cost
- Space
- Physical hardware availability
- Power – Also See Cost
- Time
- Nested virtualization
- Ease of management – Also See Time
- Aesthetics

Now What

- Build Home Services
- Harden Your Network/Segment Devices
- Replicate a Business Environment
  - Active Directory
  - Web Servers
  - File Servers
  - Database Servers
  - Segmentation/VLANs
  - Monitoring Systems
  - ….and then break stuff

Security Labs – Attack vs Defend

- Lots of CTF style options for attack
  - Vulnhub
  - HackTheBox
  - TryHackMe
  - Many, many more
- Not so much for defense…
  - Build a lab and attack it
  - Grab occasional packet captures or system images and analyze

Environmental Considerations

- **The first rule of Security Labs is Networking**
  - The second rule of security labs is networking
  - SEGMENTATION IS KEY
  - If physical, separate by VLANs and firewall them off
  - If virtualizing, ensure you have a host only network, or bridge with an interface on separate network – if possible try to use a dedicated lab system
  - You do not want something to escape your lab and target production systems – or worse – unauthorized systems
- Endpoint protection
  - In a lot of scenarios, you will either not have endpoint protection or it will be disabled
- Physical gadgets
  - Hak5 gear (BashBunny, RubberDucky, Wifi Pineapple)

Offensive Labs

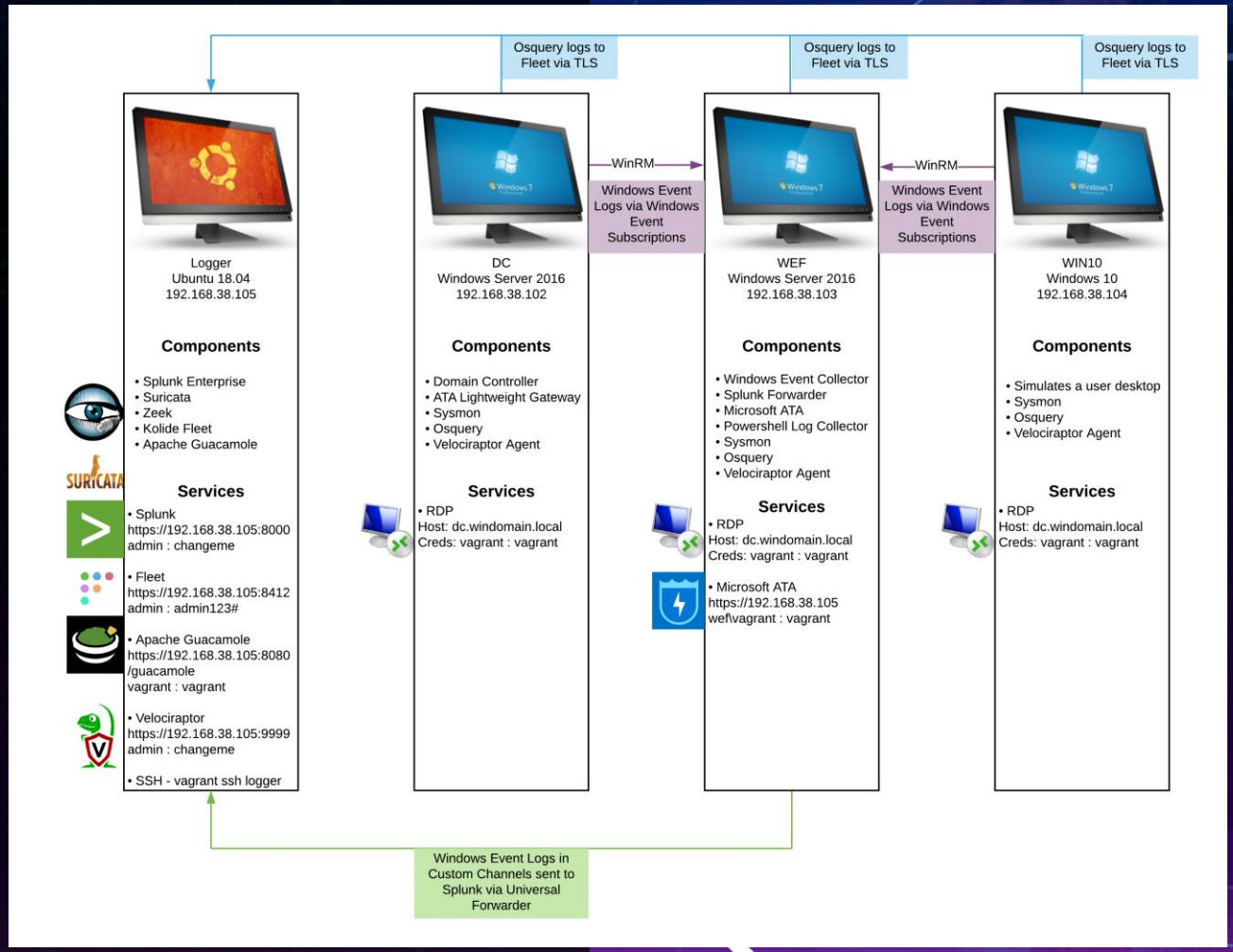
- VulnHub
  - Collection of VirtualBox and VMware virtual machines for download
  - Typically CTF style
  - Use caution, anyone can create and upload these (recommend dedicated system for this)
- HackTheBox
  - Lots of boxes, VPN in to access, challenging
- TryHackMe
  - Lots of exercises, VPN not required, guided experience
- Metasploitable – Custom VMs for use with Metasploit

Defensive Labs

- Target Machines
  - Windows Servers, Windows Endpoints, Linux Servers, Network Equipment
  - May or may not have EDR/Sysmon/EPP
- Attack Machines
  - An offensive system or a few to execute attacks from (typically Kali/Parrot)
- Analysis Machines
  - SIEM/Log Collector, IDS, Network monitoring, Malware Analysis (Cuckoo or CAPEv2)

Detection Lab

- Sadly Deprecated
- “Easy Button” for a defensive environment
- Close to reality
- Lots of resources
  - 50GB+ Storage
  - 16GB+ RAM



Security Labs - Tools

- Nmap – Network Mapper
- Wireshark – Packet Capture and Analysis
  - Malware Traffic Analysis
- OpenVAS – Vulnerability Scanner
- Volitility – Memory Forensics
- Autopsy – Disk Forensics
- CAPEv2 – Malware Analysis
- Atomic Red Team & Caldera – Atomic Indicator Generators
- MetaSploit – Exploitation Framework
- Splunk BOTS – Datasets for Analysis
- CyberChef – Data Swiss Army Knife

Thank you

Michael Miller

mmiller.netsecdev@gmail.com

Labbing Resources

- https://www.reddit.com/r/homelab/
- https://www.reddit.com/r/homelabsales/
- https://www.docker.com/
- https://linuxcontainers.org/
- https://www.vmware.com/products/workstation-pro.html
- https://www.gns3.com/
- https://www.eve-ng.net/
- https://www.netacad.com/courses/packet-tracer
- https://mikrotik.com/
- https://www.proxmox.com/en/
- https://www.freenas.org/
- https://www.pfsense.org/
- https://www.osboxes.org/
- https://pi-hole.net/

Security Resources

Defensive Labbing

- https://securityonionsolutions.com/
- https://thehelk.com/intro.html
- https://github.com/splunk/botsv3
- https://detectionlab.network/
- https://www.malware-traffic-analysis.net/training-exercises.html
- https://letsdefend.io/
- https://cyberdefenders.org/labs/
- https://dfirmadness.com/
- https://github.com/stuxnet999/MemLabs
- https://thehive-project.org/
- https://wazuh.com/
- https://www.velocidex.com/
- https://aboutdfir.com/education/challenges-ctfs/

Offensive Labbing

- https://www.vulnhub.com/
- https://www.hackthebox.eu/
- https://tryhackme.com/
- https://information.rapid7.com/download-metasploitable-2017.html
- https://github.com/rapid7/metasploitable3
- https://atomicredteam.io/
- https://caldera.mitre.org/