BUILDING HOME LABS FOR FUN & CAREER DEVELOPMENT

MICHAEL MILLER

MANAGER, INFORMATION SECURITY & RISK – PLATFORM ENGINEERING @ CARDINAL HEALTH

$>WHOAMI

- IT/Cybersecurity over 10 years
  - Cybersecurity, Network Administration, Windows/Linux Server Administration, Web App Development
  - Telecommunications, Healthcare, Consulting, Manufacturing
  - Worked with businesses ranging from <$1M to >$100B (Currently work for Fortune 20 company)
- A.A.S. – Network Administration & Computer Programming @ NSCC
- Finishing B.S. – Cybersecurity & Information Assurance @ WGU
- CCSP, SSCP, CEH, ECES, CySA+, Security+, Network+, A+, and various vendor certs
- Participate in InfraGard, ISSA, (ISC)2, Advisory Board for NSCC, CAMO 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 just software (e.g. running something like XAMPP)
  - Can be a container/VM (Docker/LXC or Virtual Box/VMware/Parallels)
  - Full enterprise network with switching, VLANs, hypervisor, NAS, etc
- Why
  - Why not, it’s fun!
  - Learn new concepts or technologies (networking, system administration, programming, pen testing, etc)
  - Test out ideas or changes without effecting a production environment
  - Implement services at home (e.g. PiHole, Plex, NextCloud, GitLab, Network monitoring, SIEM, Syncthing, etc)
  - Resume/skills building

HOW – SOFTWARE, CONTAINERIZATION, OR VIRTUALIZATION

- Software
  - XAMPP
  - Installing services directly on a home PC or laptop (e.g. Apache, MySQL, Metasploit, Plex)
- Containerization (OS Level Virtualization)
  - BSD Jails
  - Docker
  - LXC
  - OpenVZ
  - Kubernetes
- Type 2 Virtualization
  - VMware Workstation/Fusion
  - VirtualBox
  - Parallels (Mac)
  - Hyper-V
  - WSL
- Network Virtualization
  - GNS3
  - Cisco Packet Tracer
  - Cisco VIRL

HOW - HARDWARE

- Network gear
  - MikroTik
  - Ubiquiti
  - Old stuff off eBay/auctions
- Servers/Storage
  - Old computers
  - Single board computers (Rasberry Pi)
  - Old stuff off eBay/auctions
- Dedicated Type 1 Hypervisor
  - ProxMox VE
  - VMware ESX
  - Hyper-V
  - Xen
- Dedicated network storage
  - FreeNAS
  - UnRAID
  - Synology
  - QNAP

HOW - CLOUD

- Azure
  - Dreamspark
- GCP
- AWS
- VPC
  - Digital Ocean
  - Linode

HURDLES/CAVEATS

- Cost
- Space
- Physical hardware availability
- Power
- Time
- Nested virtualization
- Ease of management

INSPIRATION

- r/Homelab
- PiHole
- Media server (Plex/Emby)
- Personal Cloud (NextCloud)
- Multiple device synchronization (Syncthing)
- Monitoring systems (Zabbix, Zeek, Security Onion, SIEM)

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

- Networking, networking, 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
- 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)

VULNHUB

- Collection of VirtualBox and VMware virtual machines for download
  - https://www.vulnhub.com/
- Typically CTF style
- Lots of cool OSCP like options
  - https://www.abatchy.com/2017/02/oscp-like-vulnhub-vms
  - https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=0
- Use caution, anyone can create and upload these (recommend dedicated system for this)

HACK THE BOX

- Amazing Website with tons of boxes to work with
- Updated all the time
- Premium options
- VPN to their environment
- https://www.hackthebox.eu/
- Open registration, used to require “hacking” your way to register

OTHER ATTACK LAB RESOURCES

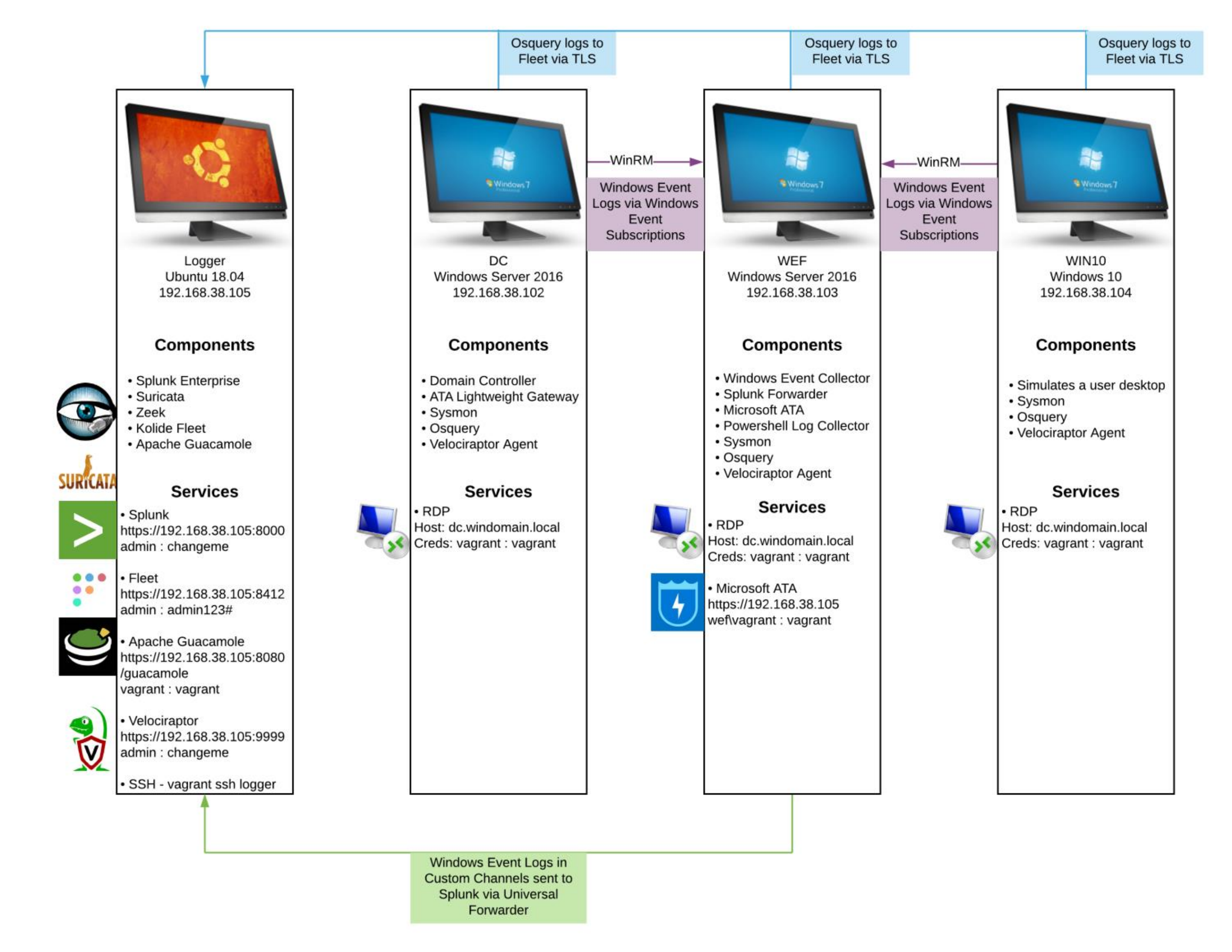
- Metasploitable
  - https://information.rapid7.com/download-metasploitable-2017.html
  - https://github.com/rapid7/metasploitable3
- Metasploit Unleashed
  - https://www.offensive-security.com/metasploit-unleashed/
- TryHackMe
  - https://tryhackme.com/
- Root Me
  - https://www.root-me.org/?lang=en

BUILDING A DEFENSE LAB

- 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)

DETECTION LAB

- "Easy Button" for a defensive environment
- Close to reality
- Lots of resources
  - 50GB+ Storage
  - 16GB+ RAM
- https://detectionlab.network/



Osquery logs to Fleet via TLS

Osquery logs to Fleet via TLS

Osquery logs to Fleet via TLS

WinRM

Windows Event Logs via Windows Event Subscriptions

WinRM

Windows Event Logs via Windows Event Subscriptions

Logger
Ubuntu 18.04
192.168.38.105

Components

- Splunk Enterprise
- Suricata
- Zeek
- Kolide Fleet
- Apache Guacamole

Services

- Splunk
https://192.168.38.105:8000
admin : changeme
- Fleet
https://192.168.38.105:8412
admin : admin123#
- Apache Guacamole
https://192.168.38.105:8080
/guacamole
vagrant : vagrant
- Velociraptor
https://192.168.38.105:9999
admin : changeme
- SSH - vagrant ssh logger

DC
Windows Server 2016
192.168.38.102

Components

- Domain Controller
- ATA Lightweight Gateway
- Sysmon
- Osquery
- Velociraptor Agent

Services

- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant

WEF
Windows Server 2016
192.168.38.103

Components

- Windows Event Collector
- Splunk Forwarder
- Microsoft ATA
- Powershell Log Collector
- Sysmon
- Osquery
- Velociraptor Agent

Services

- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant
- Microsoft ATA
https://192.168.38.105
wef\vagrant : vagrant

WIN10
Windows 10
192.168.38.104

Components

- Simulates a user desktop
- Sysmon
- Osquery
- Velociraptor Agent

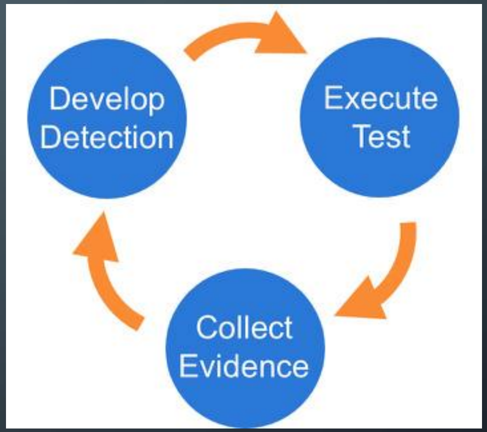
Services

- RDP
Host: dc.windomain.local
Creds: vagrant : vagrant

Windows Event Logs in Custom Channels sent to Splunk via Universal Forwarder

ATOMIC RED TEAM & CALDERA

- Atomic Indicator Generator
- Maps to MITRE ATT&CK
- https://atomicredteam.io/
- https://caldera.mitre.org/



OTHER DEFENSE TESTING METHODS

- Metasploit
- Nmap
- OpenVAS
- Wireshark
- Cobalt Strike

STATIC TESTING RESOURCES

- https://www.malware-traffic-analysis.net/training-exercises.html
- https://letsdefend.io/
- https://cyberdefenders.org/labs/
- https://dfirmadness.com/
- https://github.com/stuxnet999/MemLabs

HOME LABBING RESOURCES

- https://www.apachefriends.org/index.html
- https://www.docker.com/
- https://linuxcontainers.org/
- https://openvz.org/
- https://www.vmware.com/products/workstation-pro.html
- https://www.vmware.com/products/fusion.html
- https://www.parallels.com/
- https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/
- https://www.osboxes.org/
- https://www.gns3.com/
- https://www.gns3.com/marketplace/featured
- https://www.netacad.com/courses/packet-tracer
- https://learningnetwork.cisco.com/s/virl
- https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-cml-personal
- https://mikrotik.com/
- https://www.ui.com/

- https://www.proxmox.com/en/
- https://kb.vmware.com/s/article/2107518
- https://www.cbtnuggets.com/blog/certifications/cloud/vmware-esxi-free-vs-paid-a-look-at-license-limitations
- https://xenproject.org/
- https://www.freenas.org/
- https://www.synology.com/en-us
- https://www.qnap.com/en-us/
- https://www.pfsense.org/
- https://www.zabbix.com/
- https://pi-hole.net/
- https://nextcloud.com/
- https://about.gitlab.com/
- https://www.turnkeylinux.org/
- https://www.reddit.com/r/homelab/
- https://www.reddit.com/r/homelabsales/

DEFENSIVE SECURITY RESOURCES

- https://securityonionsolutions.com/
- https://thehelk.com/intro.html
- https://cybersecurity.att.com/products/ossim
- https://www.elastic.co/what-is/elk-stack
- https://thehive-project.org/
- https://cuckoosandbox.org/
- https://suricata.io/
- https://www.snort.org/
- https://www.ossec.net/
- https://wazuh.com/
- https://osquery.readthedocs.io/en/stable/
- https://www.velocidex.com/
- https://openedr.com/
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

QUESTIONS?

Contact: mmiller.netsecdev@gmail.com

LinkedIn: https://www.linkedin.com/in/michaelmillerdev/