How to Build a Home Lab for Infosec

Ralph May

#WHOAMI

RALPH MAY

- Full-time Pentester @ BHIS
- lots of pen testing
- I love to Automate
- Army Veteran
- Home Lab Addict

#WARNING

- This is a minefield
- Lots of opinions
- Plenty of options
- Things can get expensive
- Price in mind (enterprise)
- Lots of products I am not involved with any of them
- We're not going to talk about every option

#WHY

- Learn new software/concepts
- Test in isolated environments
- Troubleshoot problems
- Test patches
- Practice attacks
- Emulate Production
- Test Malware

#GOALS

- What do you want to solve
- What do you want to learn
- How much do you want to spend
- How much will you use it

#HOMELAB PARTS

- Network
  - Switch
  - Firewall
  - Wifi
- Storage
  - RAID
  - Storage Types
  - NAS
- Compute
  - Components
  - Form Factors

#NETWORK

- Internet
- Firewall / Router
- Switch
- Wi-Fi

#INTERNET

- Avoid Internet provider routers.
- GO for Fiber
- Bridge mode on your Modem/Router

#FIREWALL

- Packet Inspection
- IDS/IPS
- VLANs
- DNS
- IP Filtering
- Easy Management
- VPN's

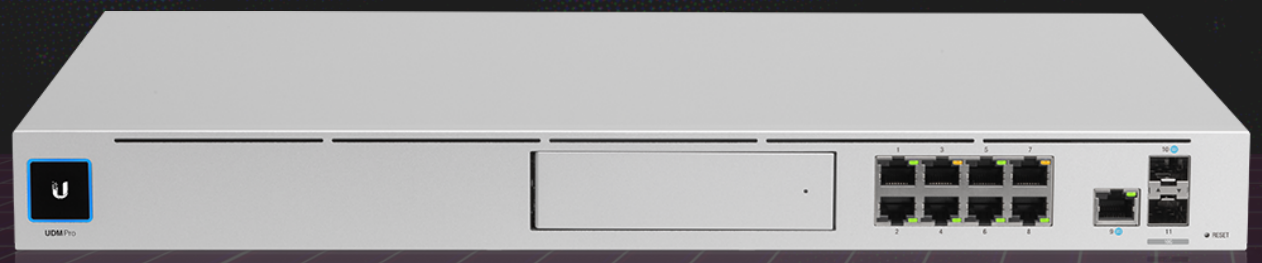
Firewalla

- Simple Configuration
- Premade hardware of different sizes
- Segmentation
- Deep Packet Inspection
- VPN

PFSense / Opensense

- Open / Source - Free
- Premade hardware & build your own
- FreeBSD based
- Plugins
- VPN

UNIFI UDM

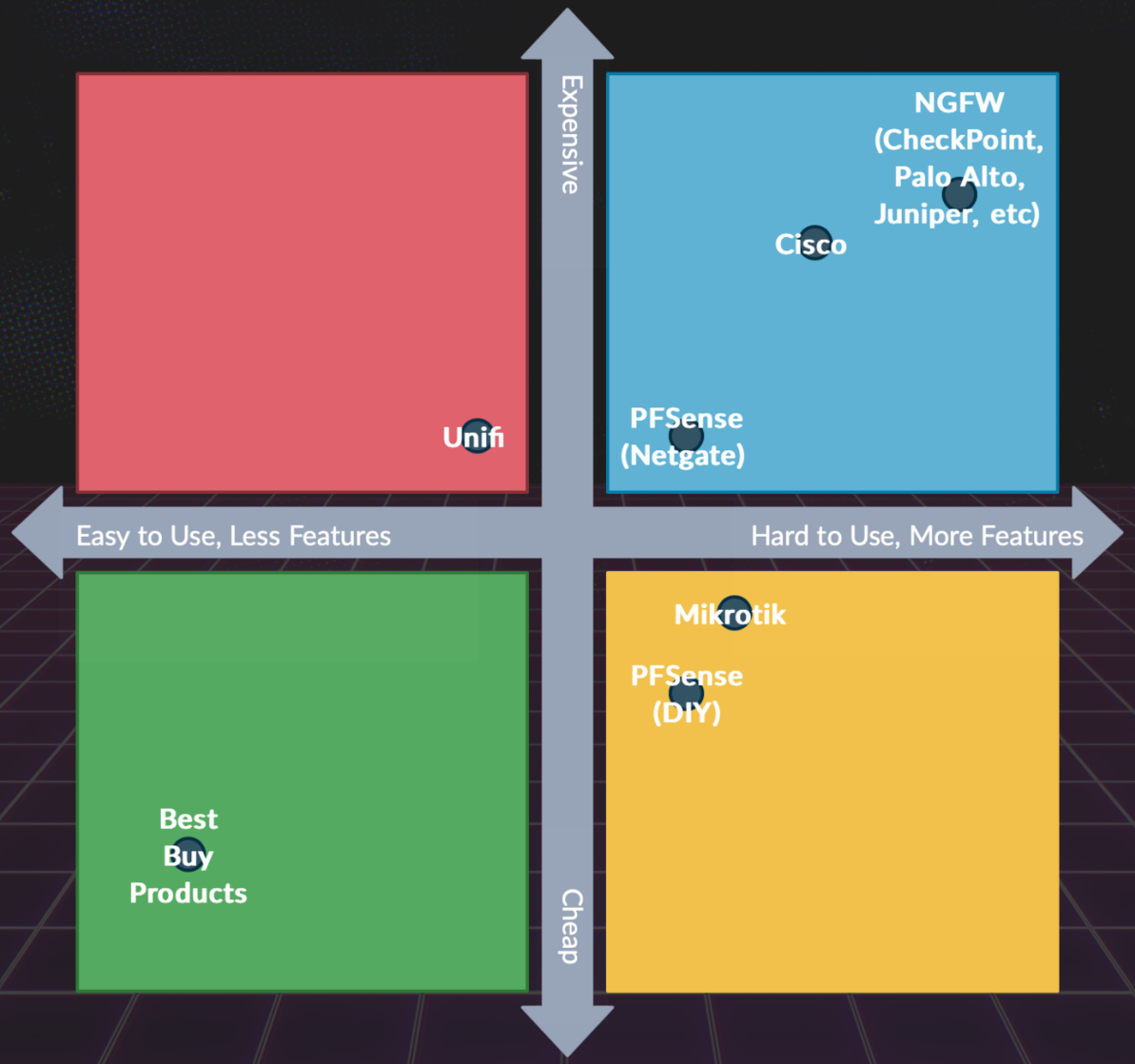


- Closed Source
- Part of the Unifi Ecosystem
- Large hardware support
- Amazing web management
- Simplicity
- Not as Feature Rich

Microtik

- Closed Source
- Router OS is Very Powerful
- Large hardware support
- Very Affordable
- Complex

#FIREWALL DIGRAM



#SWITCH

- Vlans
- Management
- Port Speed
- Size
- POE

#SWITCH OPTIONS

- Unifi
- TP Link Omada
- NetGear

#WIFI

- Speed Wifi-6
- Scale
- Management
- AP vs AP & Router

#WIFI HARDWARE

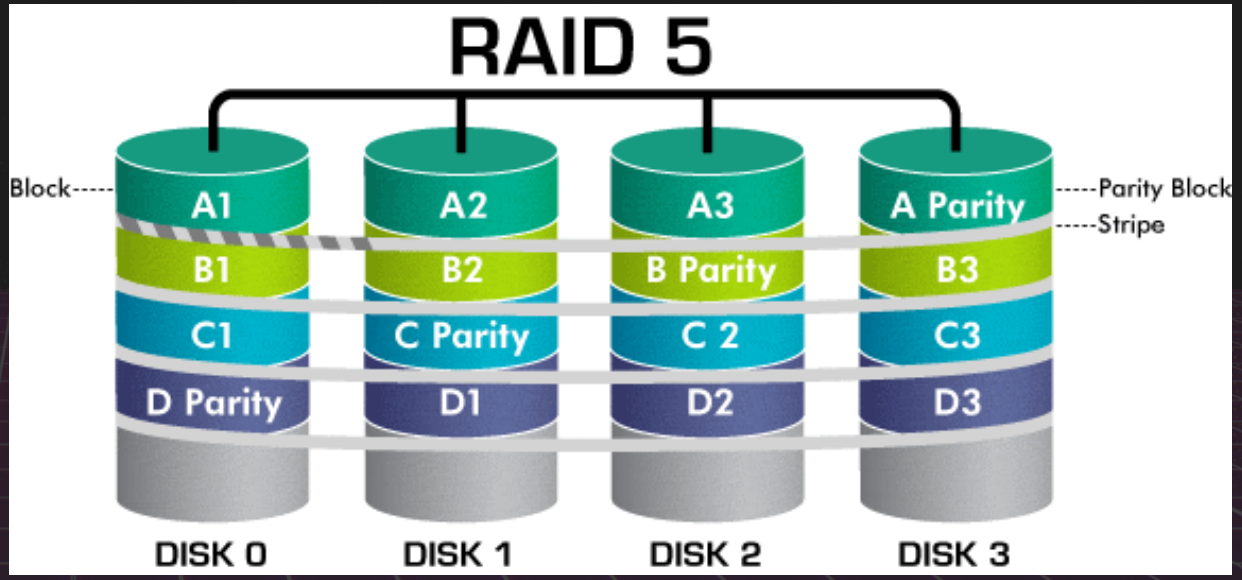
- Unifi
- TP Link Omada
- NetGear

#STORAGE

- 3.5 SATA Plater
  - High Space slow
- 2.5 SATA SSD
  - Lower Space Fast
- M.2 PCI NVME
  - The fastest / highest cost per TB
- Local Storage
- NAS

#STORAGE RAID

- Raid types
  - Software
  - Hardware
- Common Raid
  - Hardware Raid Card
  - ZFS
  - BTRFS
  - Linux MD



#STORAGE TYPES

Slow / high $ per TB

Fast

Fastest / Low & per TB

#STORAGE LOCAL VS NAS

- Local Storage
  - Fastest Read & Writes
  - Single host use
  - No network limits
  - Cheapest
- Network Storage
  - Multiple hosts
  - Network speed limits
  - Great for files

#STORAGE NAS BUILD

TrueNAS

- ZFS File System
- VM
- Docker / K3
- ISCSI
- NFS/SMB

UNRAID

- Unraid / XFS
- VM
- Docker
- NFS/SMB

#STORAGE NAS BUY

- Hardware Support
- Higher cost / Vs Building
- Simplicity
- Docker
- VM
- Low Power

#COMPUTE

- CPU
  - x86 - 64
  - ARM
- RAM
- PCI
- GPU
- Management
- Form Factor
  - Laptop
  - Mini PC
  - Server

#COMPUTE X86-64

- General purpose CPU
- Largest OS support
- AMD / Intel Arc
- Higher Power
- Best server CPU
- high software support

#COMPUTE AMD DESKTOP

AMD Ryzen 9 5950X		Average CPU Mark
Description:		
Class: Desktop	**Socket:** AM4	
Clockspeed: 3.4 GHz	**Turbo Speed:** 4.9 GHz	
Cores: 16 **Threads:** 32	**Typical TDP:** 105 W	
Cache Size: L1: 1024 KB, L2: 8.0 MB, L3: 64 MB		
Other names: AMD Ryzen 9 5950X 16-Core Processor		
CPU First Seen on Charts: Q4 2020		
CPUmark/$Price: 83.47		
Overall Rank: 56		
Last Price Change: $549.00 USD (2022-11-19)		

45822

Single Thread Rating: 3463

Samples: 6075*

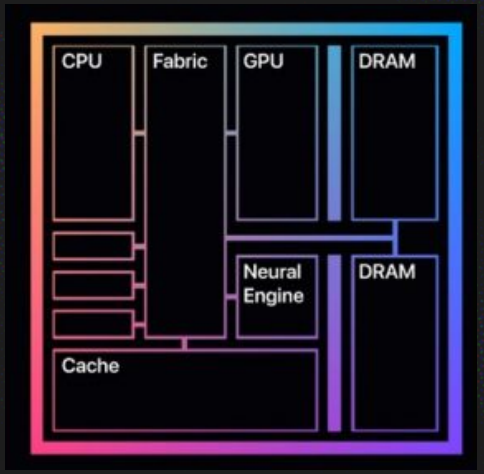
*Margin for error: Low

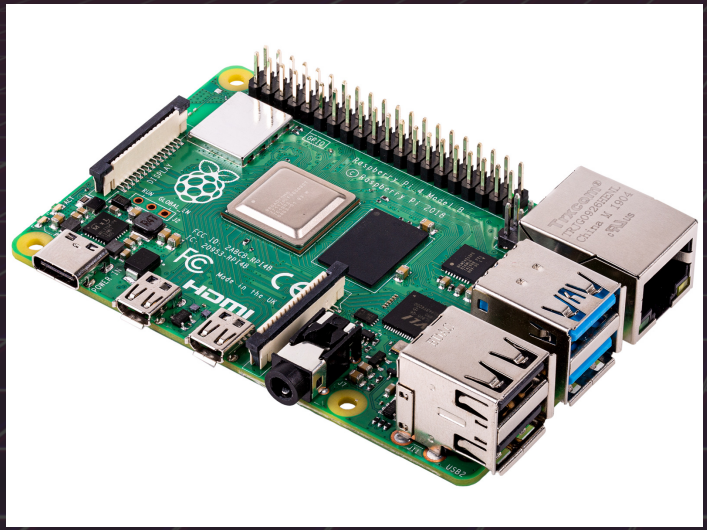
+ COMPARE

#COMPUTE AMD LAPTOP

AMD Ryzen 9 6900HX		Average CPU Mark
Description: AMD Radeon 680M		25043
Class: Laptop	**Socket:** FP7	Single Thread Rating: 3403
Clockspeed: 3.3 GHz	**Turbo Speed:** 4.9 GHz	Samples: 75*
Cores: 8 **Threads:** 16	**Typical TDP:** 45 W	*Margin for error: Low
Cache Size: L1: 512 KB, L2: 4.0 MB, L3: 16 MB		+ COMPARE
Other names: AMD Ryzen 9 6900HX with Radeon Graphics		
CPU First Seen on Charts: Q2 2022		
CPUmark/$Price: NA		
Overall Rank: 205		
Last Price Change: NA		

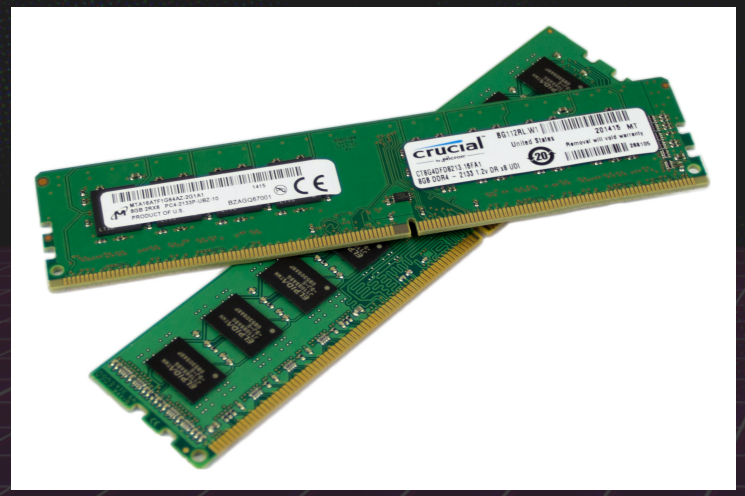
#COMPUTE ARM





- Amazing Performance per watt
- Primarily used in phones
- Mac M1/M2
- Server
- Raspberry Pi
- Limited Windows Support
- Not good for virtualization

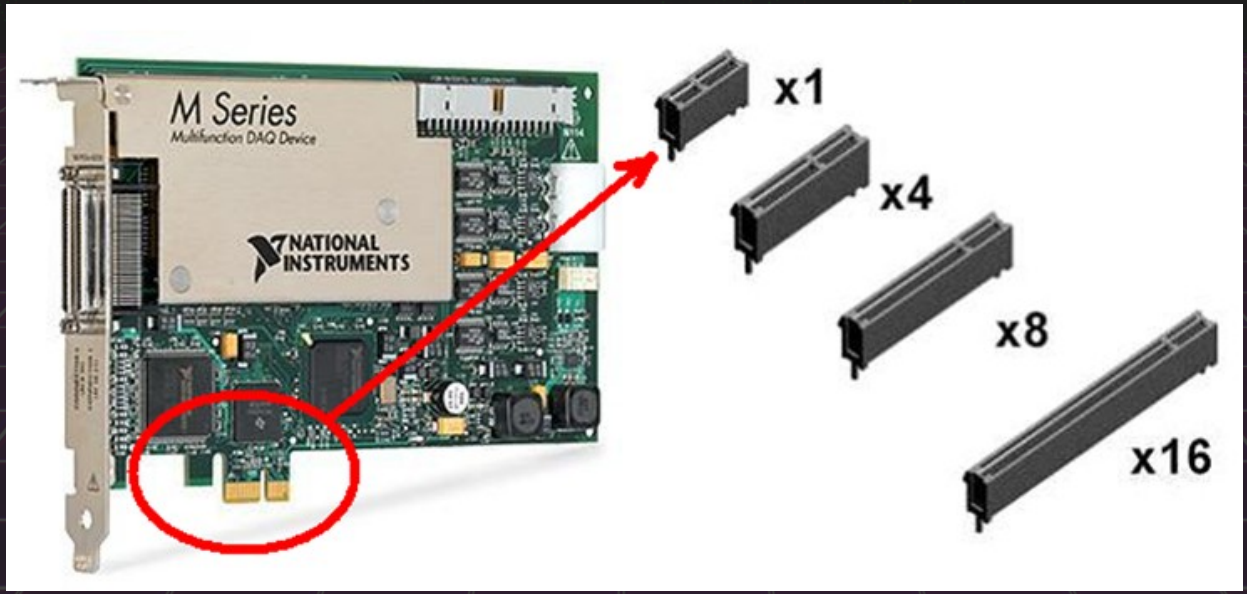
#COMPUTE RAM



- Size
  - DIMM
  - SODIMM
  - Embedded
- Speed
  - DDR3
  - DDR4
  - DDR5
- Registered
- ECC

#COMPUTE PCI

PCI Express version	Introduced	Line code	Transfer rate[i]	Throughput[i]				
				x1	x2	x4	x8	x16
1.0	2003	8b/10b	2.5 GT/s	250 MB/s	0.500 GB/s	1.00 GB/s	2.0 GB/s	4.0 GB/s
2.0	2007	8b/10b	5.0 GT/s	500 MB/s	1.000 GB/s	2.00 GB/s	4.0 GB/s	8.0 GB/s
3.0	2010	128b/130b	8.0 GT/s	984.6 MB/s	1.969 GB/s	3.94 GB/s	7.88 GB/s	15.75 GB/s
4.0	2017	128b/130b	16.0 GT/s	1969 MB/s	3.938 GB/s	7.88 GB/s	15.75 GB/s	31.51 GB/s
5.0	2019	128b/130b	32.0 GT/s[ii]	3938 MB/s	7.877 GB/s	15.75 GB/s	31.51 GB/s	63.02 GB/s
6.0 (planned)	2021	128b/130b	64.0 GT/s	7877 MB/s	15.754 GB/s	31.51 GB/s	63.02 GB/s	126.03 GB/s



#COMPUTE GPU

- Use Case
  - Password Cracking
  - Crypto Mining
  - ML/AI
  - Desktop / GUI
- Increase Cost
- Increase Power
- Increase Case Size

#COMPUTE MANAGMENT

- Extra Monitor and Keyboard
- IPMI
  - Server Motherboards
- KVM
- Pi KVM

Laptop

- Low Power
- Low CPU Performance
- Thermal Limits
- Ram Limits
- Not always online
- No Expansion
- Reuse existing hardware

Mini PC / Desktop

- Higher Power
- Consumer CPU
- Moderate to High CPU Performace
- Dedicated GPU
- Ram Limits Around 128gb
- Can Remain Online
- Some Expansion
- Reuse hardware

Server

- Highest Power
- Enterprise CPU / Mutipal
- High CPU Performace
- Dedicated GPU
- Ram Limits in the TB
- Can Remain Online
- Expansion
- Dedicated Hardware
- Redundant Hardware

Buy a Mini PC

- Small Footprint
- Lower Power
- Limited Ram
- Limited Expansion
- Easy to Cluster
- Dell Optiplex 7070 Micro

Tiny Home Lab

Build Desktop

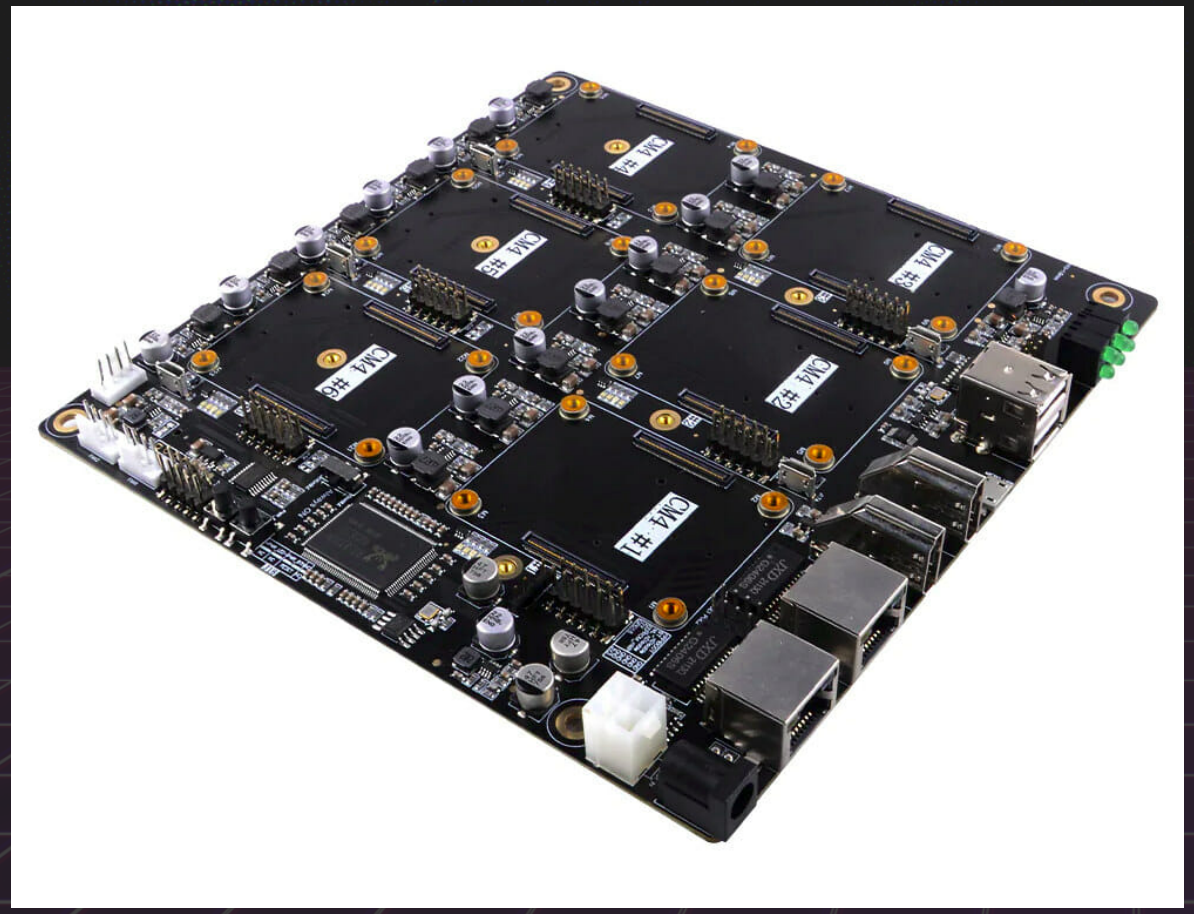
- Use existing hardware
- Consumer CPUs can be cheaper
- Low Noise
- Lots of hardware choices
- Flexibility to expand to a new case
- Focus on the performance use case
- Cheaper upgrades
- Ryzen and Intel 12 gen or lower

Buy a prebuilt server

- Pre-built enterprise hardware
- New servers can be extremely expensive
- Older hardware can be very cheap
- The Dell r730 is a good option
- Rackmount is the primary cheap choice
- Desktop options are more expensive
- Performace can be lacking

Build Server / Whitebox

- Desktop OR rackmount
- Server or Desktop CPU
- Low Noise
- Lots of hardware choices
- Flexibility to expand to a new case
- Focus on the performance use case
- Cheaper upgrades
- Ryzen and Epyc are good choices



Arm Server (Bonus)

- Kubernetes
- Low Power
- Low Noise
- DeskPi Super6C
- No VM Support
- Pi's are hard to find

#HARDWARE DEALS

- eBay
- Reddit Home Lab Sales
- Facebook Market
- Craigslist

#VERTUALIZATION / CONTAINERS

- Virtualization Type 1
  - ESXi
  - Proxmox
  - Hyper V
- Virtualization Type 2
  - VMWare Workstation
  - Virtual Box
- Containers
  - Docker
  - Kubernetes

#AUTOMATION

- Ansible
  - Host Configuration
  - Windows & Linux
  - Create Baselines
- Terraform
  - Deploy VM's
  - Proxmox
  - Esxi
  - Cloud
- Packer
  - Baseline images
  - Windows & Linux
- Vagrant
  - Local VM

HACKEROPS

Shameless plug

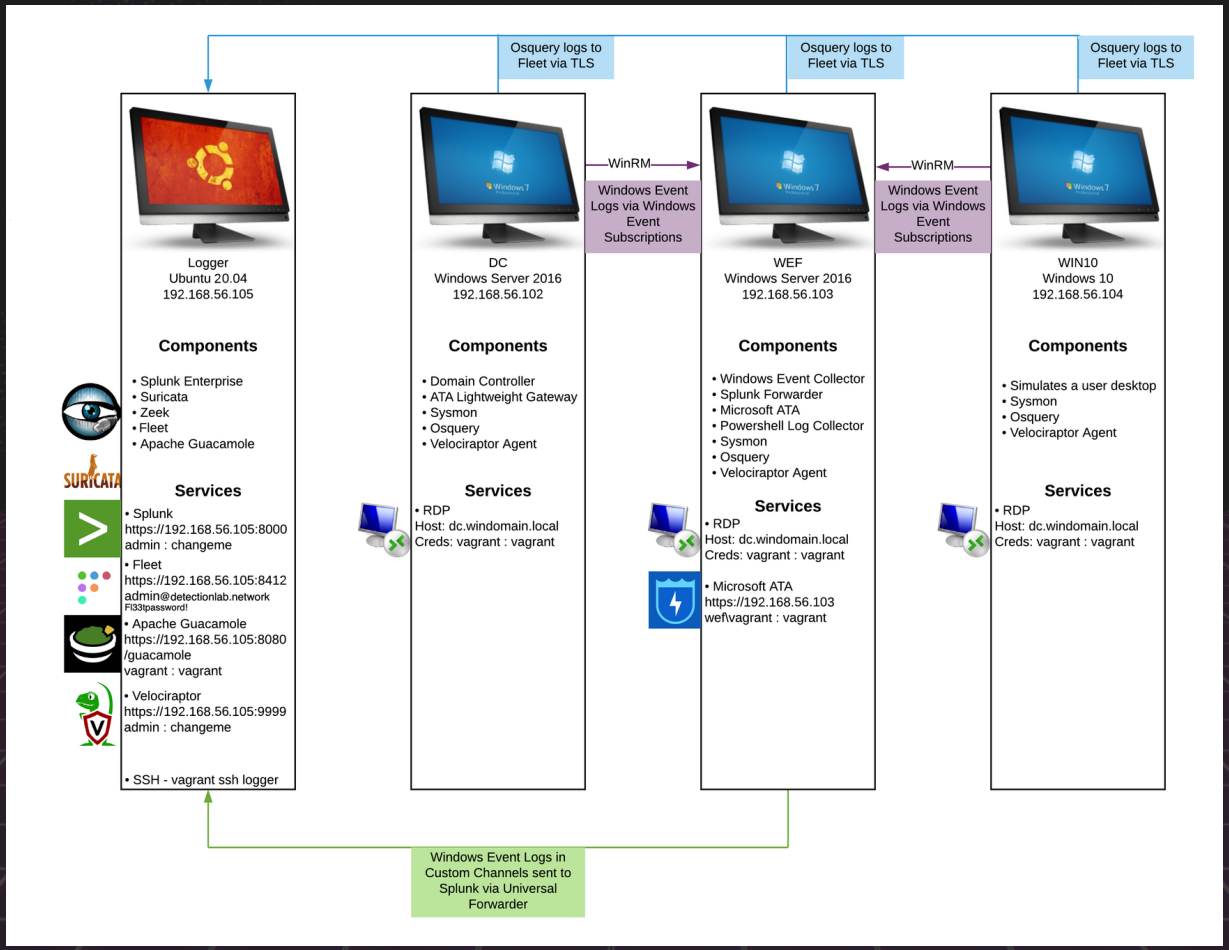
#APPLICATIONS

- AD Lab
- Detection Lab
- Self Hosted
- IDS/IPS
- Logging / Elastic

#AD LAB

- Active Directory Domain
- Test Windows Versions
- ADCS
- AD Privilege escalation
- Payload detonation
- EDR Lab Testing

#DESTECTION LAB



Detectionlab

#SELF HOSTED

- DNS - AdGuard
- Password - Bitwarden
- FIle Sharing - Nextcloud
- Anonymous email - anonaddy
- VPN - Headscale
- Proxy IAM - Pomerium
- FIle Drop - Send

SelfHosted

#IDS/IPS

- Snort
- Suricata
- Bro (Zeek)

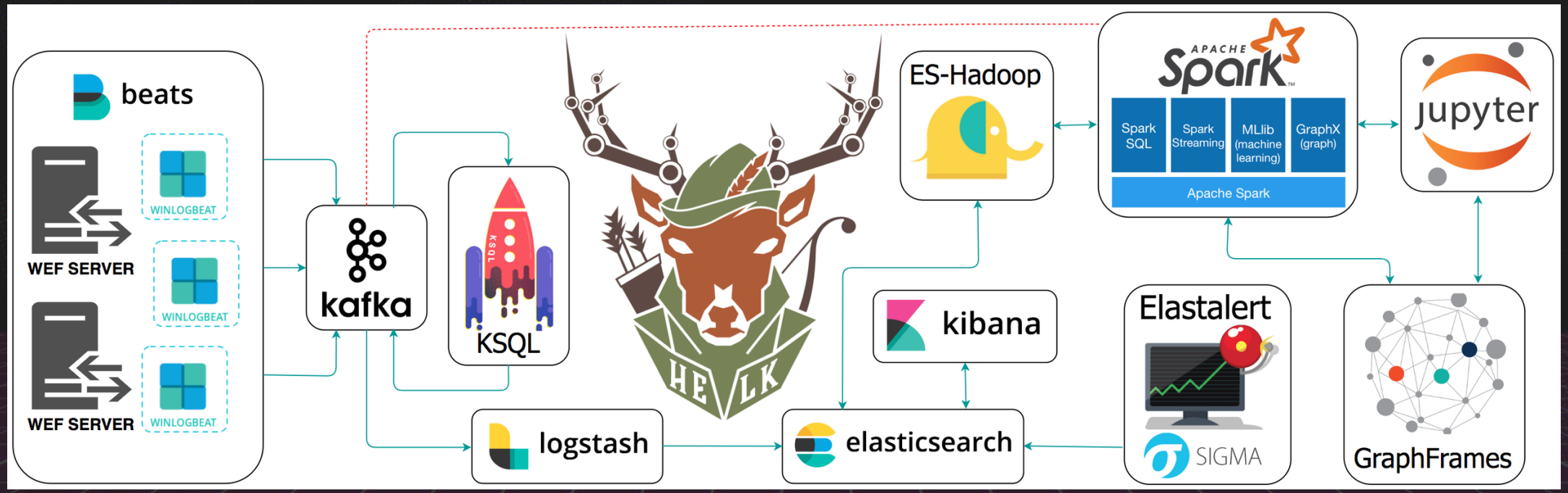
#SECURITY DISTRO

- Commando
- Kali
- Parrot Linux
- Security Onion
- Cuckoo Sandbox
- Tpot Honypot

#LOGGING

- Elastic EDR
- Elastic Search
- Logging to Elastic
- Kibana for Web Search
- Log Stash
- File Beat

#HELK


beats
WEF SERVER
WINLOGBEAT
WEF SERVER
WINLOGBEAT
WINLOGBEAT
kafka
KSQL
ES-Hadoop
APACHE Spark
Spark SQL
Spark Streaming
MLlib (machine learning)
GraphX (graph)
Apache Spark
jupyter
kibana
Elastalert
SIGMA
GraphFrames
logstash
elasticsearch
HELK

HELK

#CLOUD

- No hardware to buy or own
- Fast scaling
- Fast to setup
- More EXPENSIVE
- Limited Windows Support
- Hard to control cost
- Time Bound

#CLOUD PROVIDERS

- AWS
- Microsoft Azure
- Digital Ocean
- Vultr
- Hetzner

When should you use the cloud

- High Uptime
- Redundancy
- Short Usage
- Fast Upload
- Public IP
- Quick Deployment
- Automated Deployments
- Backups

When should you AVOID the cloud

- Lots of Windows
- High Performance requirements
- No uptime requirements
- No Automation
- High Storage Requirements

#CLOUD ON THE CHEAP

Hetzner

	vCPU	RAM	Disk space	Traffic	IPv4	Locations		
CX11	1 Intel	2 GB	20 GB	20 TB	✔	🇩🇪 🇫🇮	€ 0.0060 / hr	€ 3.79 / mo
CPX11	2 AMD	2 GB	40 GB	20 TB	✔	🇩🇪 🇫🇮 🇺🇸	€ 0.0071 / hr	€ 4.35 / mo
CX21	2 Intel	4 GB	40 GB	20 TB	✔	🇩🇪 🇫🇮	€ 0.0087 / hr	€ 5.35 / mo
CPX21	3 AMD	4 GB	80 GB	20 TB	✔	🇩🇪 🇫🇮 🇺🇸	€ 0.0120 / hr	€ 7.55 / mo
CX31	2 Intel	8 GB	80 GB	20 TB	✔	🇩🇪 🇫🇮	€ 0.0153 / hr	€ 9.70 / mo
CPX31	4 AMD	8 GB	160 GB	20 TB	✔	🇩🇪 🇫🇮 🇺🇸	€ 0.0219 / hr	€ 13.60 / mo
CX41	4 Intel	16 GB	160 GB	20 TB	✔	🇩🇪 🇫🇮	€ 0.0286 / hr	€ 17.40 / mo

#COMMUNITY

- BHIS Infosec Knowledge Share
- Homelab Reddit
- Homelab Discord

#RECAP

- Decide what you want to learn or do.
- Buy the right hardware
- Use automation
- Know when to use cloud
- There is more open source software then time.
- Join the Community

QUESTIONS

@ralphte1
@Ralphte@infosec.exchange

Ralph May