HOME SEC LAB
(FOR FUN AND !PROFIT)

Kat Fitzgerald
~~*Security Engineering Mgr*~~
Staff Security Engineer

@rnbwkat
evilkat@rnbwmail.com

1

$ whoami

- *CEO @BSidesChicago, 2019 COO @dianainitiative, CFP Chair @BSidesPGH, DefCon 3!*
- *Many years in Security, with an emphasis on Blue Teams, (former Purple), DevSecOps, IR.*
- *Based in Chicago and a natural creature of winter, you can typically find me sipping Casa Noblé Añejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos.*
- *Honeypots, Refrigerators and IoT (Internet of Threats) are a few of my favorite things!*

Love to cook!

2

DISCLAIMER

- I'm obsessed(?) with home security lab equipment, honeypots and colos
- If you want to have a life, perhaps tone it down a bit
- YMMV

3

WHY ARE WE NOT HERE

- This is not a demo of everything in my lab (yet)
- I'm not showing you all my gear (duh)
- K8s (k3s) is fun, but has been known to cause breakups

4

WHY ARE WE HERE?

- Security is fun
- Toys are fun
- I like breaking things
- I like building things
  - I like breaking things I build
- Learning never ends

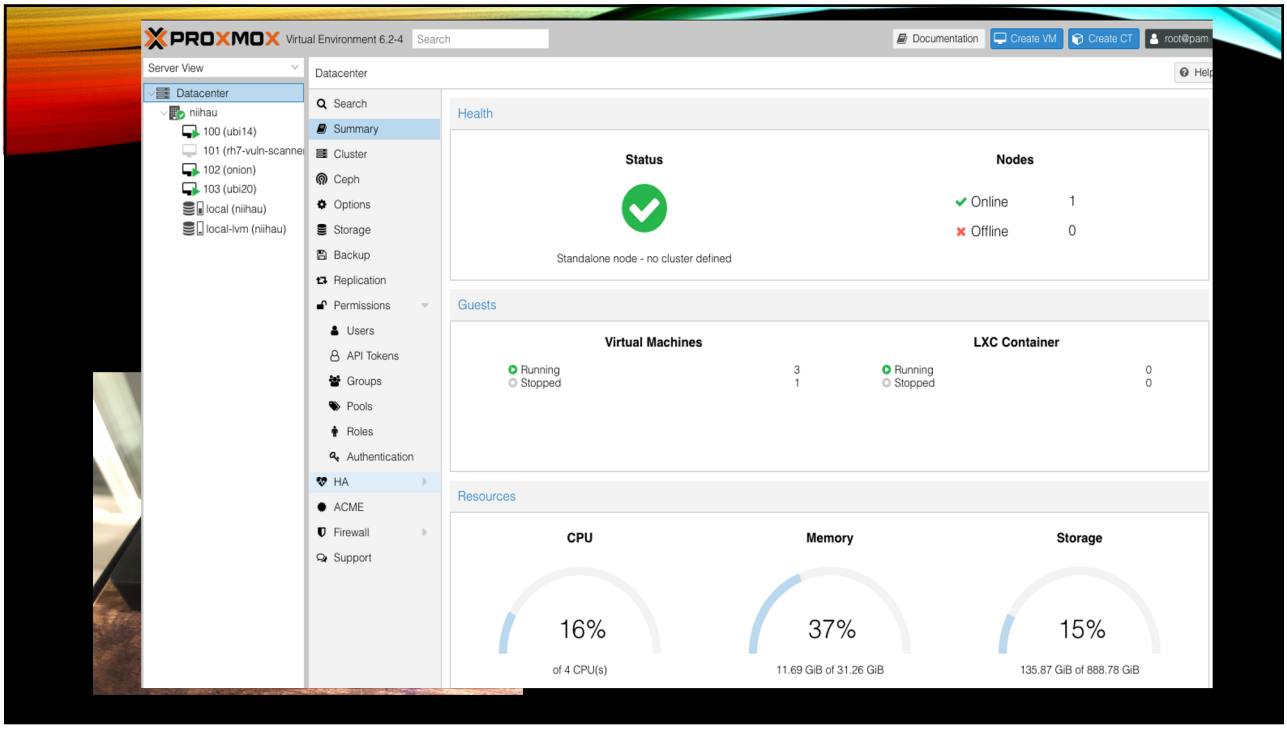
5

SOME BASICS

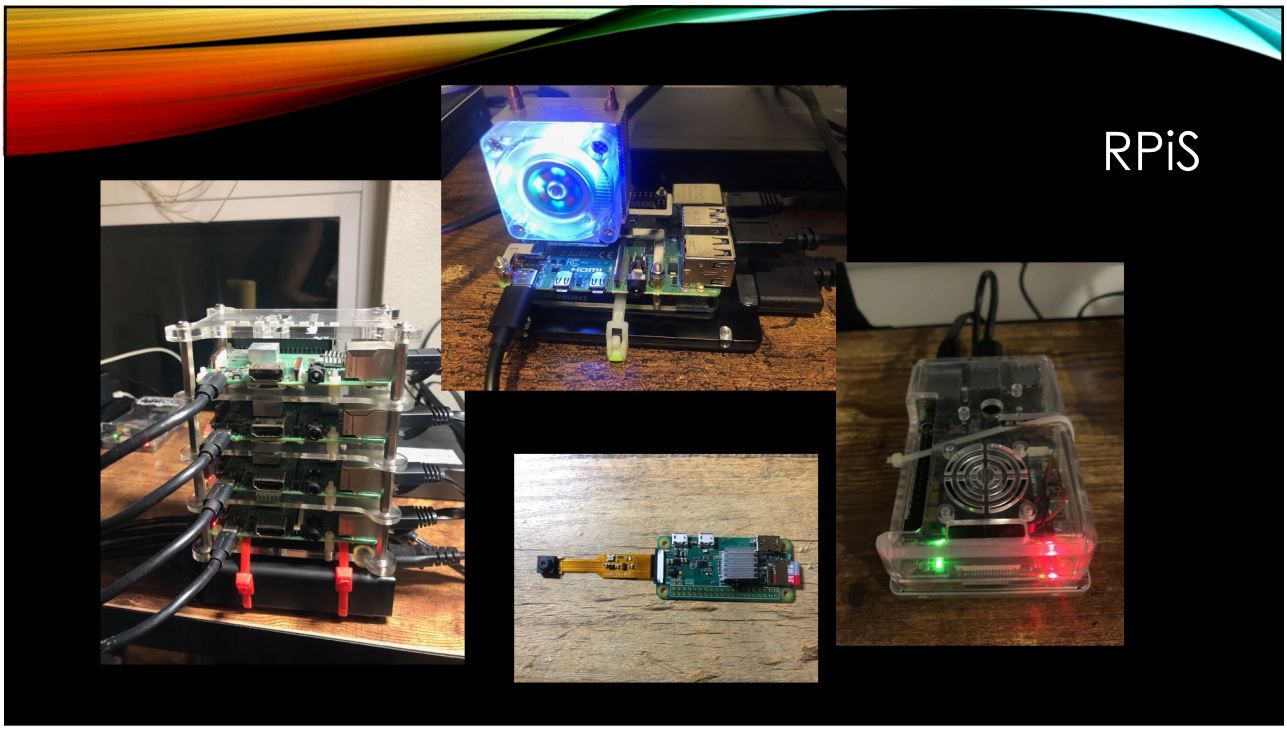
Your Lab!

- Virtualize
  - Proxmox - https://proxmox.com/en/
  - Virtualbox
- PIs
- OpenWRT - https://openwrt.org/
- OpnSense - https://opnsense.org/
- Random Bits

6


PROXMOX Virtual Environment 6.2-4
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
Datacenter
niihau
100 (ubi14)
101 (rh7-vuln-scanner
102 (onion)
103 (ubi20)
local (niihau)
local-lvm (niihau)
Search
Summary
Cluster
Ceph
Options
Storage
Backup
Replication
Permissions
Users
API Tokens
Groups
Pools
Roles
Authentication
HA
ACME
Firewall
Support
Health
Status
Standalone node - no cluster defined
Nodes
Online 1
Offline 0
Guests
Virtual Machines
Running 3
Stopped 1
LXC Container
Running 0
Stopped 0
Resources
CPU
16%
of 4 CPU(s)
Memory
37%
11.69 GiB of 31.26 GiB
Storage
15%
135.87 GiB of 888.78 GiB

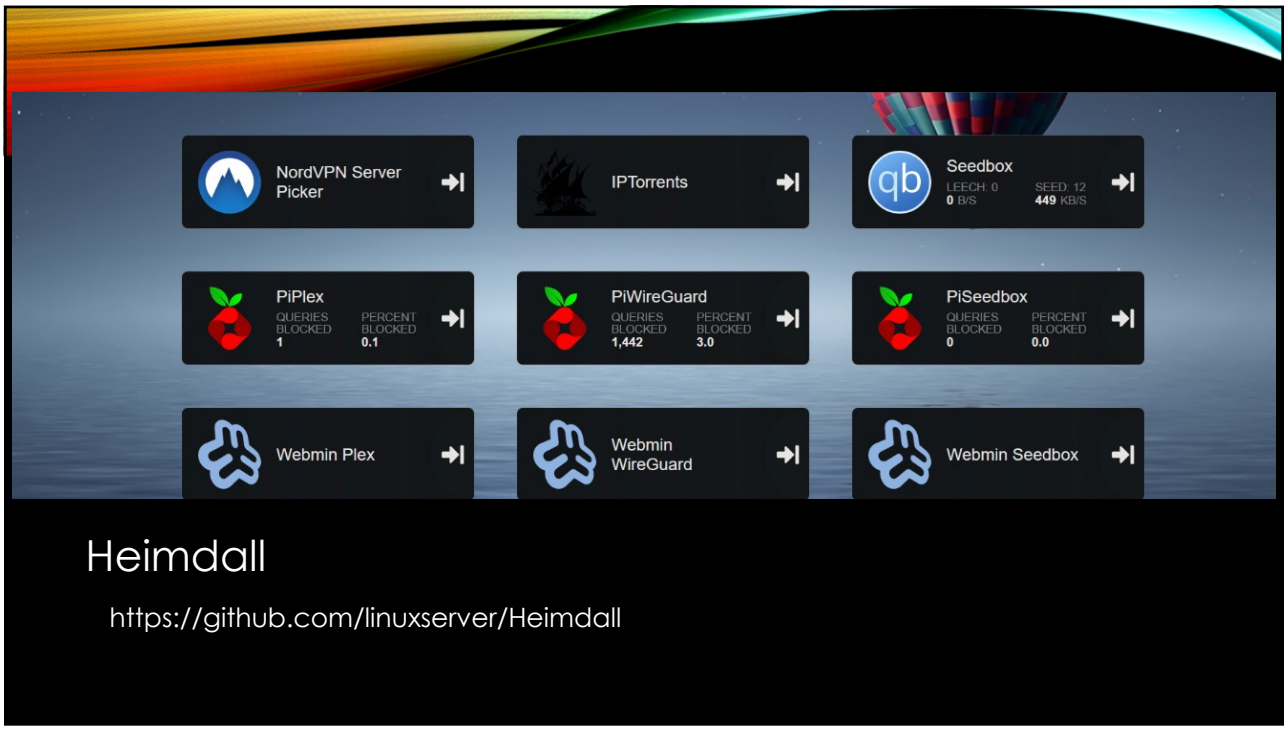
7


RPiS

8


NETWORK
192.168.2.5
NETGEAR
ProSAFE
Plus Switch
GS108E
https://openwrt.org/
https://dd-wrt.com/

9


NordVPN Server Picker
IPTorrents
Seedbox
LEECH: 0
0 B/S
SEED: 12
449 KB/S
PiPlex
QUERIES BLOCKED
1
PERCENT BLOCKED
0.1
PiWireGuard
QUERIES BLOCKED
1,442
PERCENT BLOCKED
3.0
PiSeedbox
QUERIES BLOCKED
0
PERCENT BLOCKED
0.0
Webmin Plex
Webmin WireGuard
Webmin Seedbox
Heimdall
https://github.com/linuxserver/Heimdall

10

RANDOM BITS

- eBay is your friend
- So is Amazon – sort of
- Old, new, borrowed & Blue
  - Desktops
  - Laptops
- SSDs
- PoE/PiHats
- USB/enet
- $50-$2000

11

12

OK – NOW WHAT?

- Install all the things!
- OSes come in all shapes and sizes
- Plan!
  - unplan (rePlan?)
- Don't forget Windoze
  - https://www.microsoft.com/en-us/evalcenter/
  - Snapshots (180 days)
- Security Onion or Wazuh (more in a minute)

13

A Quick Cluster - 5 minutes

- 4 nodes
  - Raspberry Pi 3 Model B Plus Rev 1.3
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2

```
$ k3sup install --ip 192.168.2.70 --user pi --context isis --local-path $HOME/.kube/config --k3s-channel latest
$ export KUBECONFIG=/Users/kat8172/.kube/config

$ kubectl get node -o wide
NAME    STATUS  ROLES   AGE     VERSION       INTERNAL-IP    EXTERNAL-IP   OS-IMAGE                    KERNEL-VERSION   CONTAINER-RUNTIME
pitop   Ready   master  2m16s   v1.19.4+k3s1  192.168.2.70   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.4.1-k3s1

$ kubectl get node -o wide
NAME    STATUS  ROLES   AGE     VERSION       INTERNAL-IP    EXTERNAL-IP   OS-IMAGE                    KERNEL-VERSION   CONTAINER-RUNTIME
pitop   Ready   master  15m     v1.19.4+k3s1  192.168.2.70   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.4.1-k3s1
izzie1  Ready   <none>  2m53s   v1.18.12+k3s1 192.168.2.71   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.3.3-k3s2
izzie2  Ready   <none>  83s     v1.18.12+k3s1 192.168.2.72   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.3.3-k3s2
izzie3  Ready   <none>  51s     v1.18.12+k3s1 192.168.2.73   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.3.3-k3s2
```

14

Let's Fix it

k3sup join --ip 192.168.2.71 --server-ip 192.168.2.70 --user pi --k3s-channel latest
k3sup join --ip 192.168.2.72 --server-ip 192.168.2.70 --user pi --k3s-channel latest
k3sup join --ip 192.168.2.73 --server-ip 192.168.2.70 --user pi --k3s-channel latest

$ kubectl get node -o wide

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	KERNEL-VERSION	CONTAINER-RUNTIME
izzie3	Ready	<none>	8m15s	v1.18.12+k3s1	192.168.2.73	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.3.3-k3s2
izzie1	Ready	<none>	10m	v1.19.4+k3s1	192.168.2.71	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1
pitop	Ready	master	23m	v1.19.4+k3s1	192.168.2.70	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1
izzie2	Ready	<none>	8m47s	v1.19.4+k3s1	192.168.2.72	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1

$ kubectl get node -o wide

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE	KERNEL-VERSION	CONTAINER-RUNTIME
izzie1	Ready	<none>	10m	v1.19.4+k3s1	192.168.2.71	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1
pitop	Ready	master	23m	v1.19.4+k3s1	192.168.2.70	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1
izzie2	Ready	<none>	9m3s	v1.19.4+k3s1	192.168.2.72	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1
izzie3	Ready	<none>	8m31s	v1.19.4+k3s1	192.168.2.73	<none>	Raspbian GNU/Linux 10 (buster)	5.4.72-v7+	containerd://1.4.1-k3s1

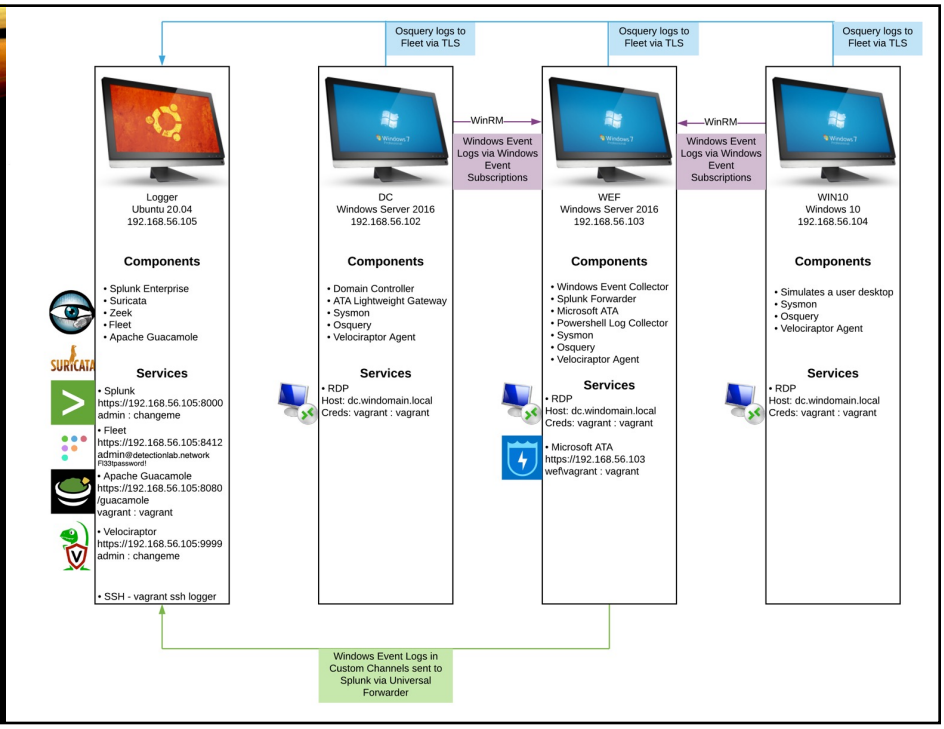
15

NOW WHAT PART 2

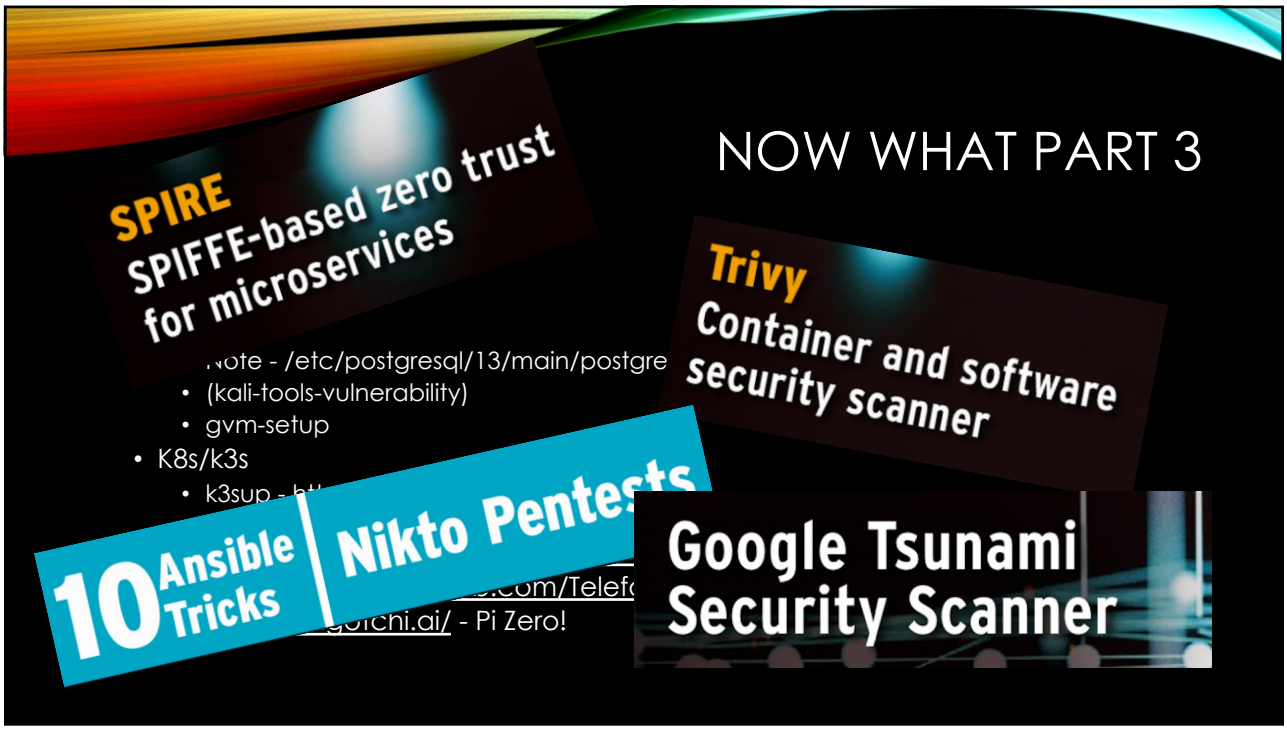
- VulnHub - https://www.vulnhub.com/
- Metasploitable 2 & 3
- Detection Lab! - https://www.detectionlab.network
  - Proxmox Deployment!
- WebGoat - https://owasp.org/www-project-webgoat/
- JuiceShop - https://owasp.org/www-project-juice-shop/
- Home Assistant - https://www.home-assistant.io/
  - HomePwn - https://github.com/Telefonica/HomePWN
- SDR!! - https://github.com/luigifcruz/pisdr-image
  - Ok, wifi too

16

Detection Lab



17



18

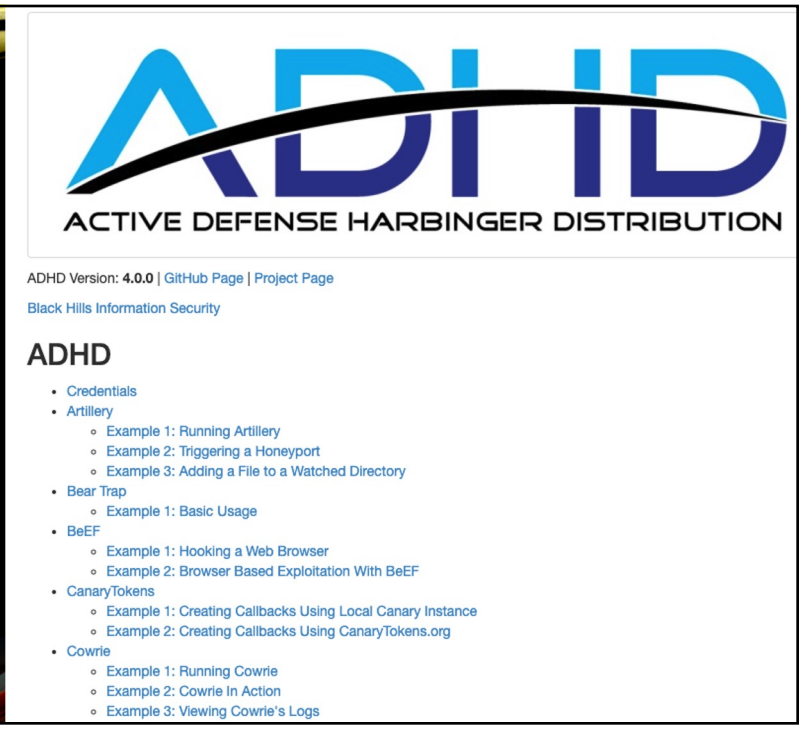
HONEYPOTS!

- OpenCanary -- https://opencanary.readthedocs.io/en/latest/
- Adhd – https://www.activecountermeasures.com/free-tools/adhd/
- Honey Badger -- https://github.com/adhdproject/honeybadger (GEO!)
- Community Honey Network -- https://communityhoneynetwork.readthedocs.io/en/stable/
- Honeypi -- https://trustfoundry.net/honeypi-easy-honeypot-raspberry-pi/
- Dshield -- https://github.com/DShield-ISC/dshield
- Canarytokens -- https://canarytokens.org/generate
- WebThings -- https://iot.mozilla.org/docs/gateway-getting-started-guide.html
- T-pot -- https://github.com/dtag-dev-sec/tpotce
- Twisted-honeypot -- https://github.com/lanjelot/twisted-honeypots
- PIs w/lights -- https://github.com/mattymcfatty/HoneyPi
- Lots more -- https://github.com/paralax/awesome-honeypots

- What about the "Real Thing"? Hmmmm..

19

ADHD



20

Date	Time	Source	Source Port	Target	Target Port	Protocol
2020-11-19	00:16:59	110.154.181.126	14649	192.168.100.100	23	6
2020-11-19	00:17:26	74.120.14.37	54522	192.168.100.100	23	6
2020-11-19	00:17:31	167.248.133.92	64123	192.168.100.100	23	6
2020-11-19	00:17:31	167.248.133.40	39580	192.168.100.100	23	6
2020-11-19	00:17:31	45.129.33.5	56294	192.168.100.100	23	6
2020-11-19	00:18:03	192.241.217.154	44838	192.168.100.100	23	6
2020-11-19	00:18:31	64.64.104.10	15188	192.168.100.100	23	6
2020-11-19	00:18:43	185.175.93.14	49700	192.168.100.100	23	6
2020-11-19	00:19:14	83.97.20.35	55995	192.168.100.100	23	6

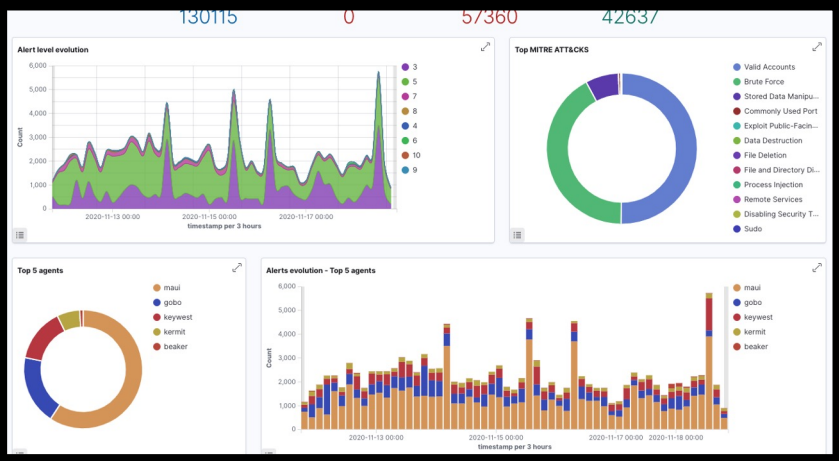
Showing 1 to 100 of 11,920 entries Previous 1 2 3 4 5 … 120 Next

DSHIELD
5 MINUTES!

21

MONITORING

WAZUH

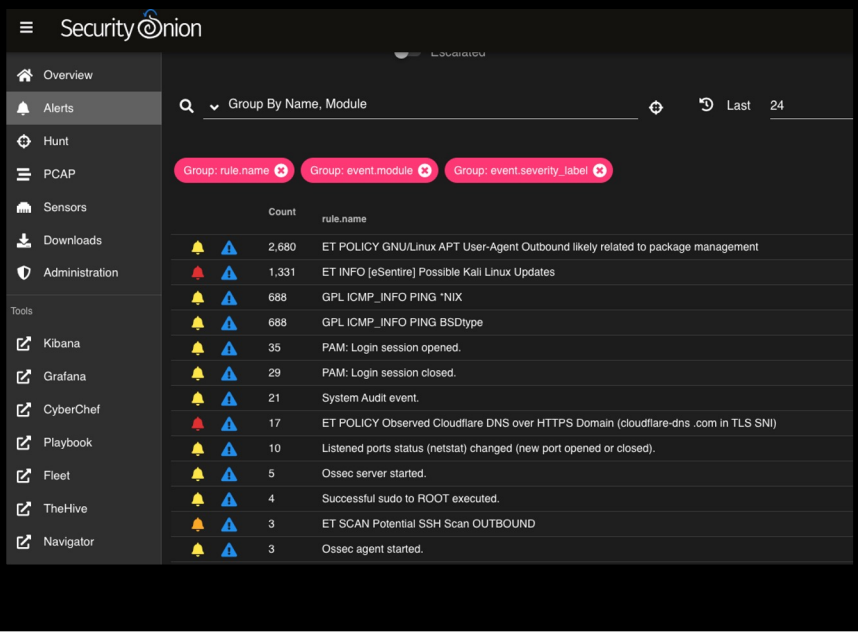



```
curl -sO https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

22

MONITORING

SECURITYONION



23

HP DEPLOYMENT

- Plan, Plan, Plan!
  - Low, Medium, ~~High~~
  - Honeypots, Honeyports, Honeytokens, Honeycreds
  - Customization <- *Ding ding ding!*
    - Real vs Self-Signed Certs
    - Actual Applications
  - HIDS / OSSEC / Wazuh / SIEM
    - Rules! Tuning

- Where?
  - Server Farms
  - Cloud Storage
  - IoT (Shodan is your friend!!)
    - https://shodan.io
  - DMZ (Guest WiFi)
  - MX, DNS
  - PoS
  - WP, Rpi, VMs, VPS

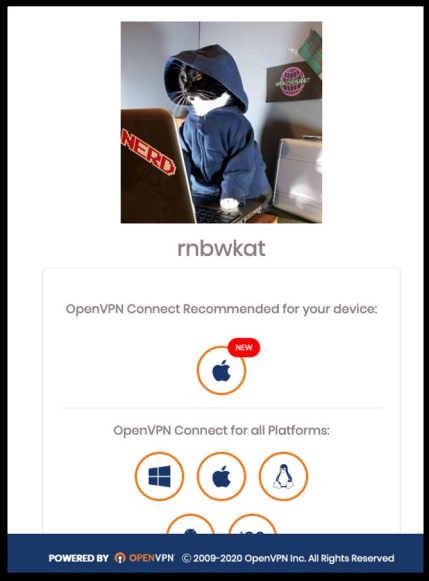
24

WHAT IS IT?

```
# uname -a
Linux RT-AC5300 2.6.36.4brcmarm #1 SMP PREEMPT Fri Oct 18 16:13:51 CST 2019
armv7l ASUSWRT
# df
Filesystem           1K-blocks      Used Available Use% Mounted on
rootfs                   40960     40960         0 100% /
/dev/root                40960     40960         0 100% /
devtmpfs                257456         0    257456   0% /dev
tmpfs                   257600       944    256656   0% /tmp
/dev/mtdblock4           65536      2064     63472   3% /jffs
```

25

WHAT IS IT?



26

TAKEAWAYS

- It's Playtime!
  - The beauty of virtualization
  - Don't forget about containers/proxmox
- There is no right or wrong
- Start small / build on it
  - Break it – build it – break it again
- You can get sucked in

27

Kat Fitzgerald

@rnbwkat
@rnbwkat@infosec.exchange

evilkat@rnbwmail.com

BSIDES CHICAGO

THANK YOU!!!

28