ERROR 404: EXPERIENCE NOT REQUIRED (WHEN YOU HAVE A HOMELAB)

Kat Fitzgerald evilkat@rnbwmail.com

github.com/rnbwkat/presents
rnbwkat@infosec.exchange
rnbwkat.bsky.social
youtube.com/@rnbwkatandtequila
(first episode being recorded in July)

theunfrostedfiles.com
sashatheflamingo.xyz

1

BSides Global Steerco, Lead BSidesChicago, CFP Chair BSidesPGH, BSidesSEA SpkrOps

Based in Chicago, IL and a natural creature of winter, you can typically find me sipping Grand Mayan Extra 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.
(Although my neighbors may disagree)

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

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

6

SOME BASICS

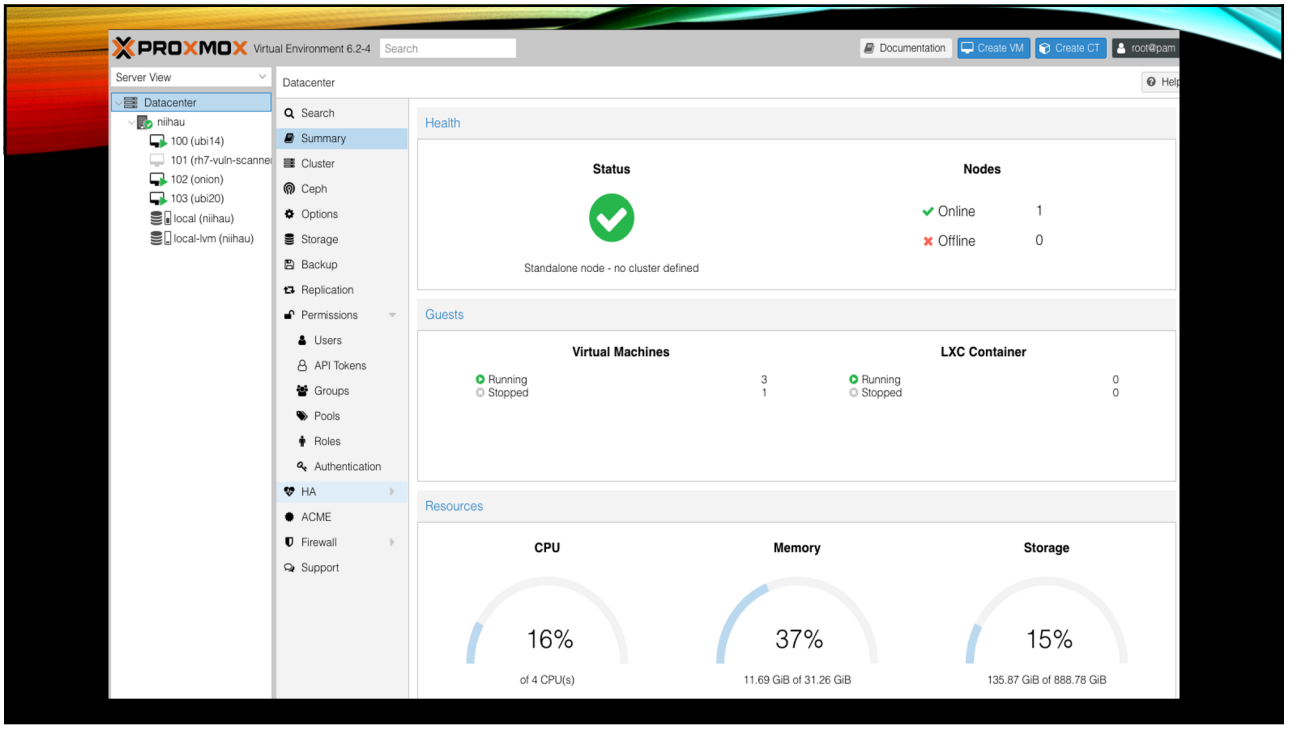
Your Lab!

- Virtualize
  - Proxmox - proxmox.com/en
  - Virtualbox – virtualbox.org
  - UTM - github.com/utmapp/UTM
- Pis
- OpenWRT - openwrt.org
- OpnSense - opnsense.org

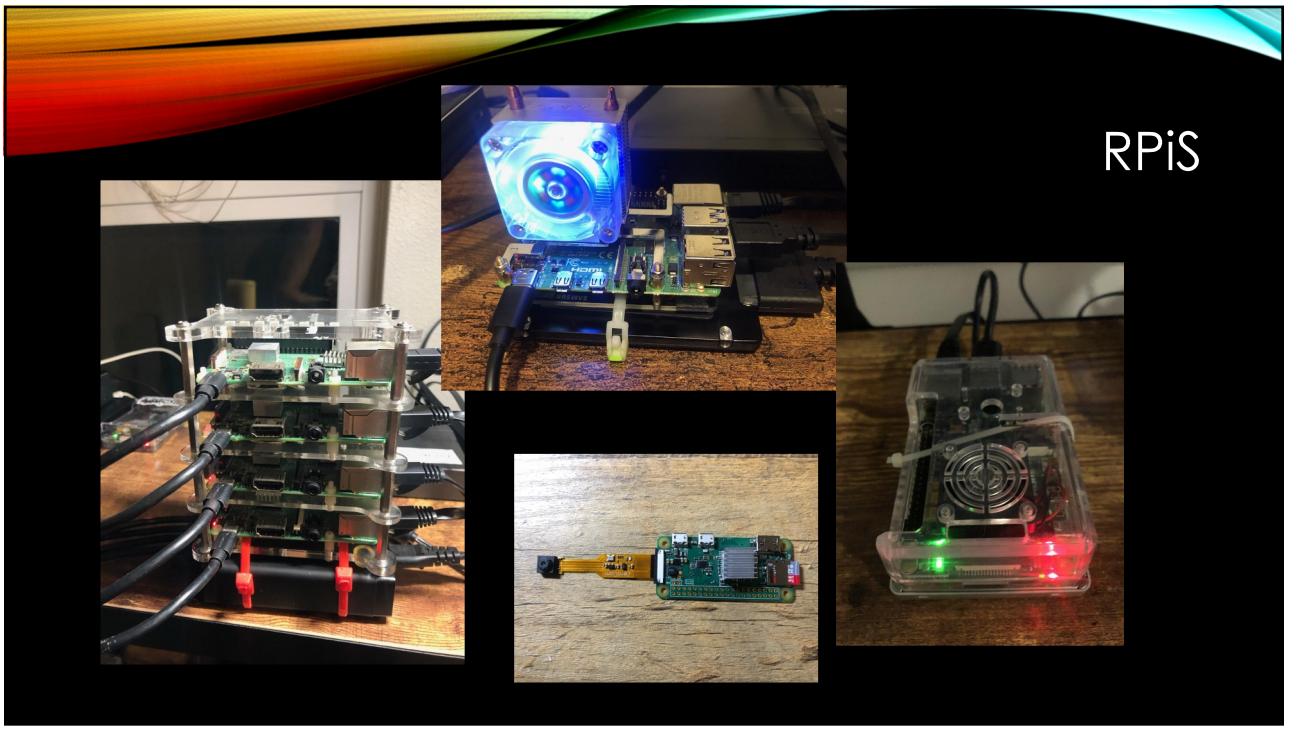
7

VIRTUALIZE!

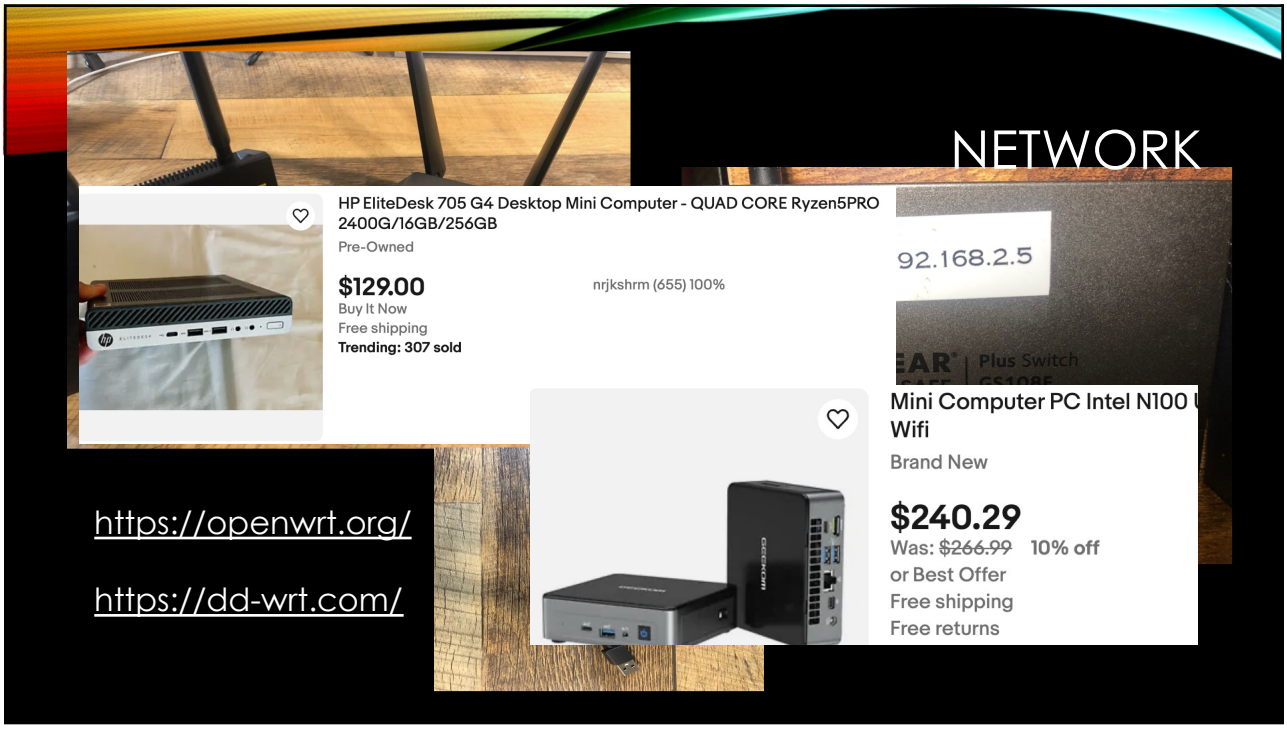
8


PROXMOX Virtual Environment 6.2-4
Search
Documentation
Create VM
Create CT
root@pam
Server View
Datacenter
Datacenter
niihau
100 (ubi14)
101 (rh7-vuln-scanne
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

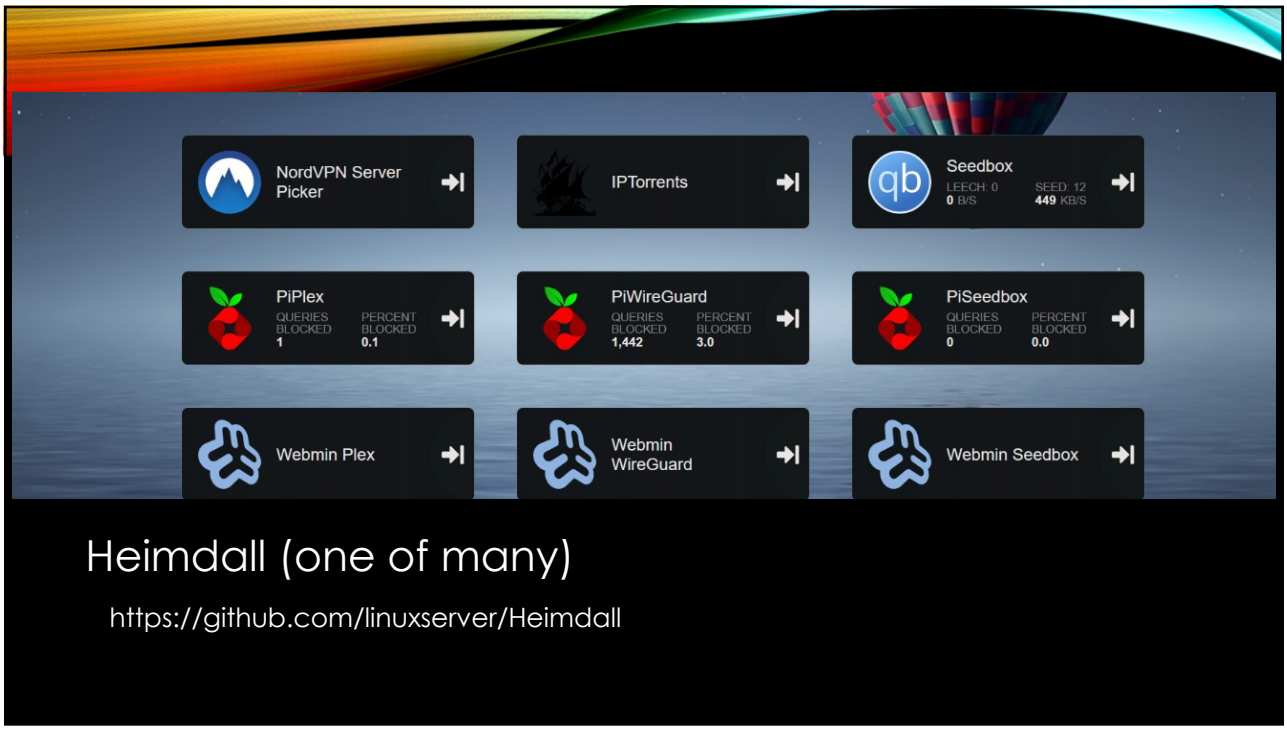
9


RPiS

10


NETWORK
HP EliteDesk 705 G4 Desktop Mini Computer - QUAD CORE Ryzen5PRO 2400G/16GB/256GB
Pre-Owned
$129.00
Buy It Now
Free shipping
Trending: 307 sold
nrjkshrm (655) 100%
92.168.2.5
Mini Computer PC Intel N100
Wifi
Brand New
$240.29
Was: $266.99 10% off
or Best Offer
Free shipping
Free returns
https://openwrt.org/
https://dd-wrt.com/

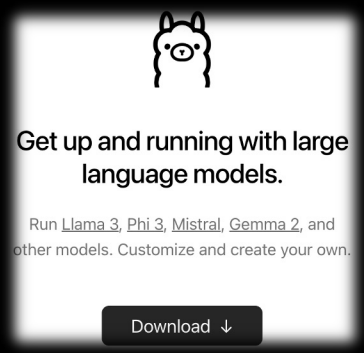
11


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 (one of many)
https://github.com/linuxserver/Heimdall

12

OK – NOW WHAT?

- Install all the things!
- OSes come in all shapes and sizes
- Ollama! ollama.com
- Don't forget Windoze
  - www.microsoft.com/en-us/evalcenter/
  - Snapshots (180 days)
- Monitoring!!! (Wazuh - more in a minute)



14

LLaMA + Suricata logs

- Install Ollama
  - curl -fsSL https://ollama.com/install.sh | sh

```
echo "Summarize these Suricata logs. Focus on unusual traffic or patterns." | \
cat - <(tail -n 100 /var/log/suricata/eve.json) | ollama run llama3
```

Between 14:00 and 14:10 UTC, host 192.168.1.42 generated over 100 DNS queries to subdomains of dns.exfiltrator.org.

Many of the query names contained unusually long, base64-encoded strings, suggesting DNS tunneling activity.

The destination was a public resolver (208.110.32.27) and not a local DNS server.
Behavior is consistent with low-rate data exfiltration via DNS covert channel.
Recommendation: Isolate host, investigate process making queries, and block outbound DNS to untrusted domains.

15

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
```

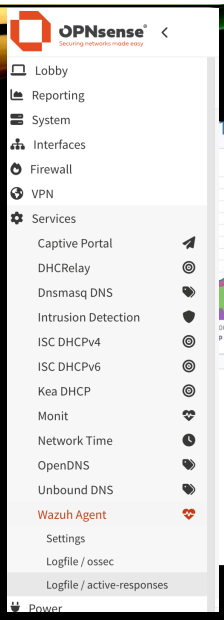
```
$ kubectl get node -o wide
NAME    STATUS   ROLES    AGE    VERSION      INTERNAL-IP    EXTERNAL-IP   OS-IMAGE                         KERNEL-VERSION   CONTAINER-RUNTIME
pitop   Ready    master   2m16s  v1.19.4+k3s1   192.168.2.70   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+      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

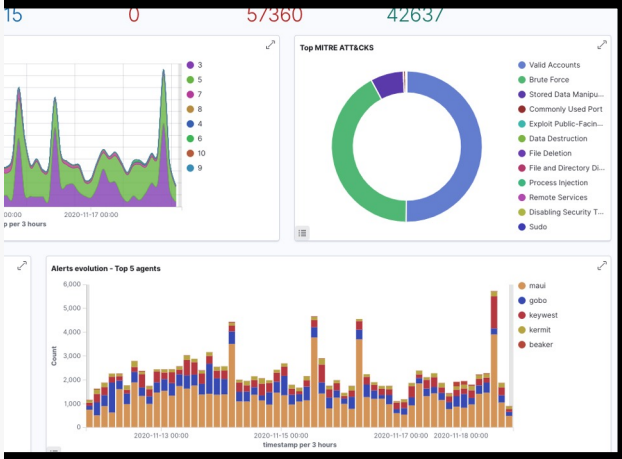
```
$ kubectl get node -o wide
NAME     STATUS   ROLES    AGE    VERSION      INTERNAL-IP    EXTERNAL-IP   OS-IMAGE                         KERNEL-VERSION   CONTAINER-RUNTIME
pitop    Ready    master   15m    v1.19.4+k3s1   192.168.2.70   <none>        Raspbian GNU/Linux 10 (buster)   5.4.72-v7+       containerd://1.4.1-k3s1
izzie1   Ready    <none>   2m3s   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
```

16

MONITORING

wazuh.com





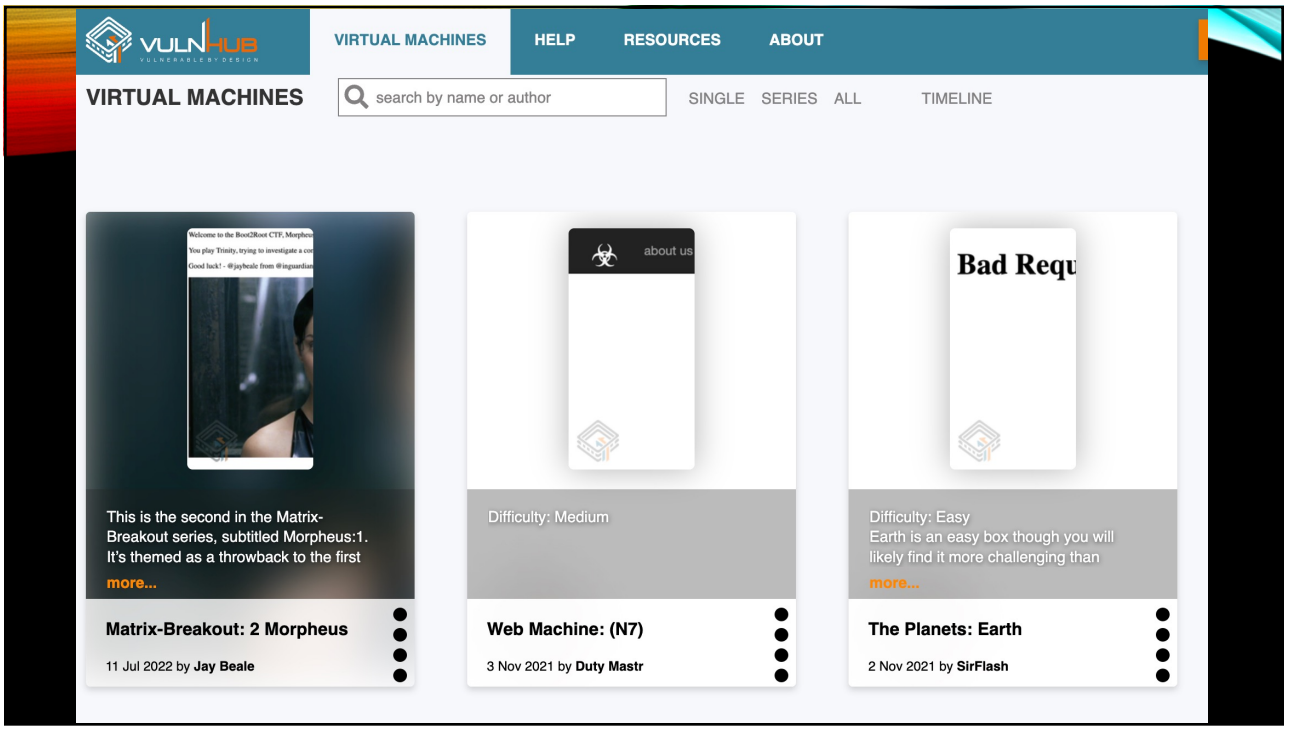

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

18

NOW WHAT PART 2

- VulnHub - www.vulnhub.com
- Metasploitable 2 & 3
- owasp.org/projects/
  - WebGoat - owasp.org/www-project-webgoat
  - JuiceShop - owasp.org/www-project-juice-shop
  - Mapping - owasp.org/www-project-amass
- Home Assistant - www.home-assistant.io
  - HomePwn - github.com/Telefonica/HomePWN
- SDR!! - github.com/luigifcruz/pisdr-image

19

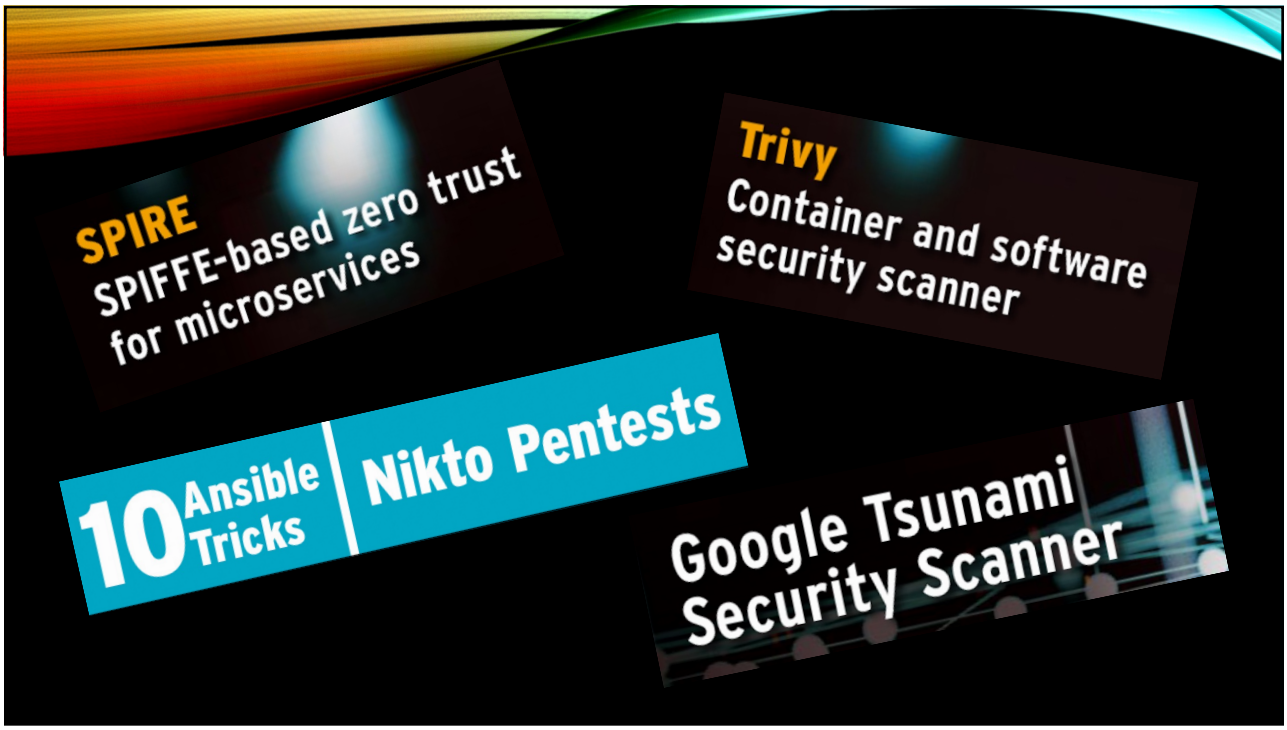


20

NOW WHAT PART 3

- Parrot OS
  - Kali
- Tenable
- HomePwn - github.com/Telefonica/HomePWN
- pwnagotchi.ai/ - Pi Zero!

21



22

Homelab AI Nodes – Project Overview

Project	Description	Core Hardware	Tools/Notes
SashaCam 5000	A next-gen AI surveillance node built on the Raspberry Pi AI Kit (M.2 HAT+ + Hailo-8 module).	Raspberry Pi 5, M.2 HAT+, Hailo-8, Pi Camera Module	YOLOv5 model, Hailo TFLite runner, image-to-alert pipeline
SashaSec Core	A real-time threat detection node powered by Suricata, Wazuh, and a Coral USB Accelerator.	Raspberry Pi 5, Coral USB Accelerator, USB/NVMe SSD	Suricata config, Wazuh rules, Coral-enhanced log summarizer

23

More Random "Now Whats"

Train an LLM to analyze logs, detect attacks, and generate incident reports

- Set up Wazuh + Zeek + Suricata for log collection.
- Feed logs into a local LLM model (Llama 3, GPT-4, or ??)
- Ask your AI SOC analyst things like:
  - *Have there been any brute-force attempts in the last 24 hours?*
  - *Summarize attack trends over the past week.*

Build a honeypot framework that auto-evolves to trick attackers

- Most honeypots get fingerprinted quickly
  - What if your honeypot was smart enough to change itself dynamically?
  - Welcome to *Cyber-Deception as a Service (CDaaS)*
    - Deploy **Kubernetes honeypots** that randomly shift attack surfaces
    - Rotate fake **misconfigurations** over time (e.g., "accidentally" exposing a fake AWS key)

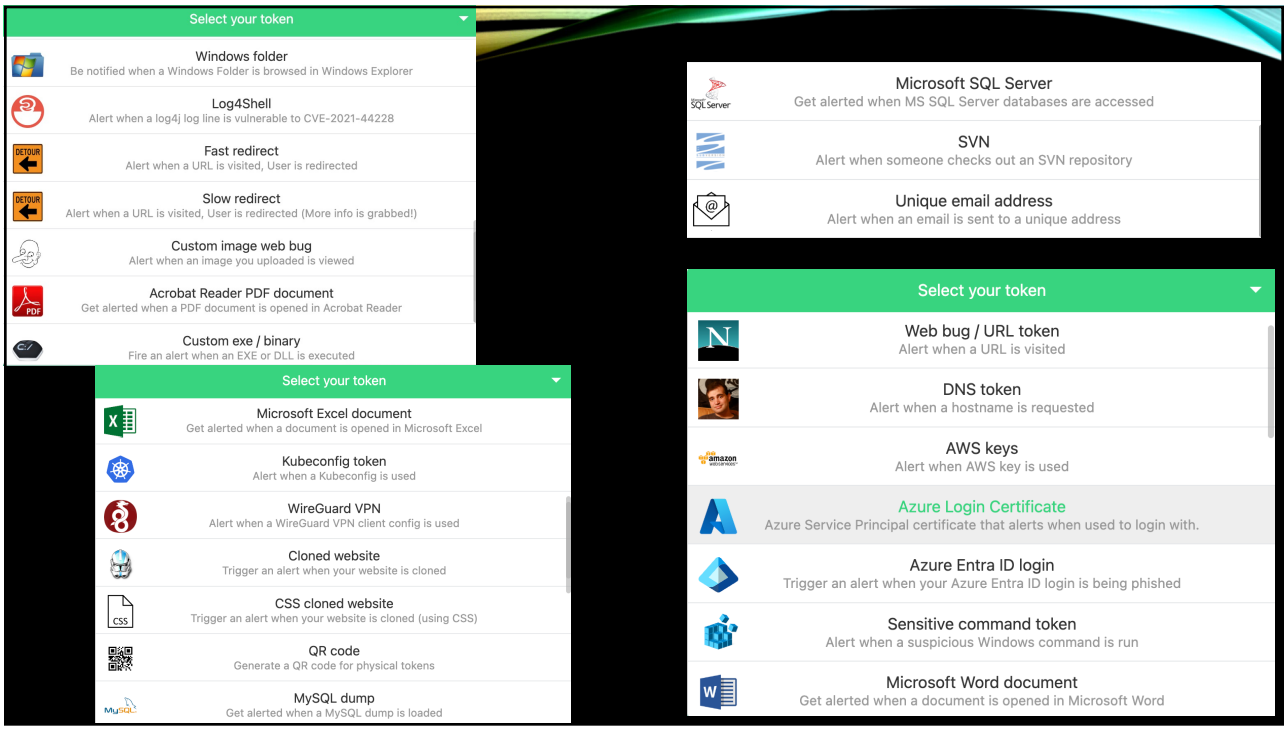
24

HONEYPOTS!

- OpenCanary -- opencanary.readthedocs.io/en/latest/
- ADHD – www.activecountermeasures.com/free-tools/adhd/
- Honey Badger -- github.com/adhdproject/honeybadger (GEO!)
- Community Honey Network -- communityhoneynetwork.readthedocs.io/en/stable/
- Honeypi -- trustfoundry.net/honeypi-easy-honeypot-raspberry-pi/
- Dshield -- github.com/DShield-ISC/dshield
- Canarytokens -- canarytokens.org/generate
- T-pot -- github.com/dtag-dev-sec/tpotce
- Lots more -- github.com/paralax/awesome-honeypots

- Personal Favorite – Honey "Data" in mysql/MSsql exposed to Internet

25



26

27

Resume Sample

Technical Expertise

- I have cultivated a robust home security lab environment, enabling hands-on exploration and experimentation with cutting-edge cybersecurity tools and techniques. My experience includes thorough malware analysis, where I dissect samples to uncover behavioral patterns, isolate indicators of compromise (IOCs), and strategize effective mitigation tactics.
- I bring proficiency in penetration testing, adept at identifying and exploiting vulnerabilities across diverse systems, networks, and applications to fortify defenses proactively. Additionally, I excel in vulnerability research, consistently uncovering security flaws within software, firmware, and hardware components. My expertise extends to Linux hardening, implementing stringent measures to safeguard Linux-based environments from potential threats.
- Complementing these skills, I possess a strong foundation in incident response methodologies, network security protocols, and cryptographic algorithms, coupled with proficiency in scripting languages like Python and Bash for automation and custom tool development in cybersecurity operations.

28

Resume Sample 2

Technical Expertise

- **Home Security Lab:** Dedicated setup at home for hands-on research and testing of cybersecurity tools and techniques.
  - **Malware Analysis:** *Proficient in analyzing malware samples to understand behavior, identify indicators of compromise (IOCs), and develop mitigation strategies.*
  - **Penetration Testing:** *Experience in conducting penetration tests to identify and exploit vulnerabilities in systems, networks, and applications.*
  - **Vulnerability Research:** *Skilled in researching and discovering security vulnerabilities in software, firmware, and hardware components.*
  - **Linux Hardening:** *Expertise in hardening Linux-based systems to enhance security posture and mitigate potential threats.*
- **Additional Skills:** Familiarity with incident response procedures, network security protocols, and cryptographic algorithms. Proficient in scripting languages such as Python and Bash for automation and tool development in cybersecurity operations.

29

Resume Sample 3

Technical Expertise

Home Security Lab: Dedicated setup for hands-on security research, network segmentation, and threat detection.

- **Intrusion Detection & Prevention:** Configured **Suricata** to monitor and analyze network traffic, identifying potential threats and anomalies in real time.
- **Firewall & Network Segmentation:** Deployed **OPNsense** with VLANs to **isolate IoT devices**, reducing attack surface and mitigating lateral movement risks.
- **Network Traffic Analysis:** Developed rules and alerting mechanisms to **detect suspicious activity from IoT devices**, enhancing network visibility.
- **Threat Hunting & Incident Response:** Used Suricata logs to investigate security events, refine detection rules, and **improve automated threat response strategies**.
- **Security Automation & Scripting:** Utilized **Python and Bash** to automate log analysis, rule updates, and alert tuning for optimized security operations.

30

Resume Sample 4

Technical Expertise

- **AI-Driven Security Lab:** Built a fully operational home lab integrating AI tools with traditional security infrastructure to enhance threat detection, analysis, and response.
- **AI Integration & SOC Automation:** Deployed LLaMA 3 locally to summarize Suricata and Wazuh logs, enabling natural-language incident reports and reducing analyst alert fatigue.
- **Edge AI Inference:** Implemented Raspberry Pi AI Kit (Hailo-8) to run YOLOv5 models for real-time object detection and anomaly flagging in surveillance environments.
- **Threat Detection & Log Correlation:** Combined Suricata, Zeek, and Wazuh to monitor, correlate, and triage alerts from multiple honeypots and segmented network zones.
- **SOC Tools Deployment:** Configured alert pipelines, dashboards, and alert tuning using open-source tools like Wazuh, Elastic, and custom scripts.
- **Security AI Prompt Engineering:** Developed effective prompts and automation scripts to guide local LLMs in daily summarization and pattern recognition of security data.
- **Automation & Custom Tooling:** Leveraged Python and Bash to automate data ingestion, enrichment, and AI-driven response recommendations.

31

the forgotten training/Learning

"Learning from a great teacher is discovery, not studying."

- antisyphontraining.com
  - *Ranging from Noobs to most Senior*
  - *Free and Pay-what-you-can*
- tcm-sec.com
  - *Beginner to advanced and all kinds of discounts throughout the year*
- tryhackme.com & academy.hackthebox.com
  - *Gamified trainings – I do both myself!*

32

KEY 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
  - Make a plan!

33

Thank You!

Kat Fitzgerald

github.com/rnbwkat/presents
rnbwkat@infosec.exchange
rnbwkat.bsky.social
YT/@rnbwkatandtequila

evilkat@rnbwmail.com

infosec.exchange/@sashatheflamingo
@sashatheflamingo.bsky.social

sashatheflamingo.xyz !!!!!!

34