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

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.*

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 We Aren't Here

- This is not a demo of everything in my lab (yet)
- I'm not showing you all my gear (duh)

5

Why We Are Here!

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

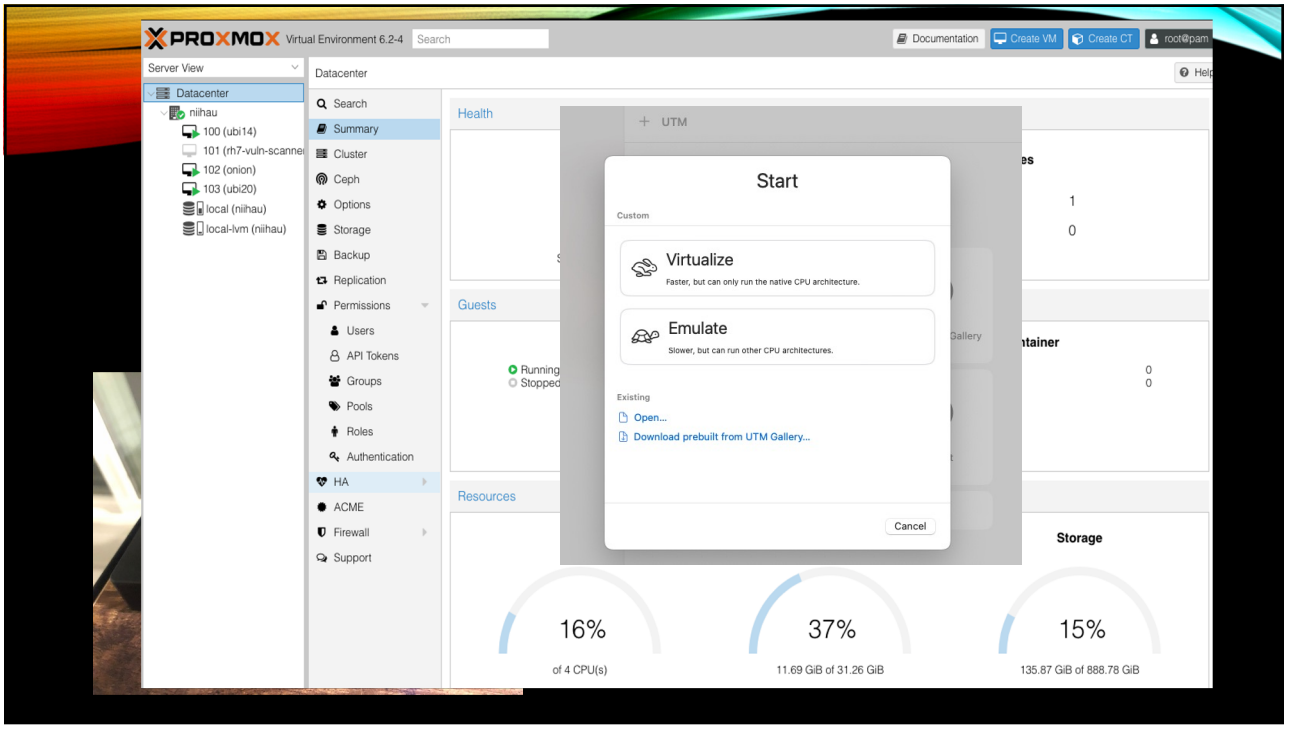
6

SOME BASICS

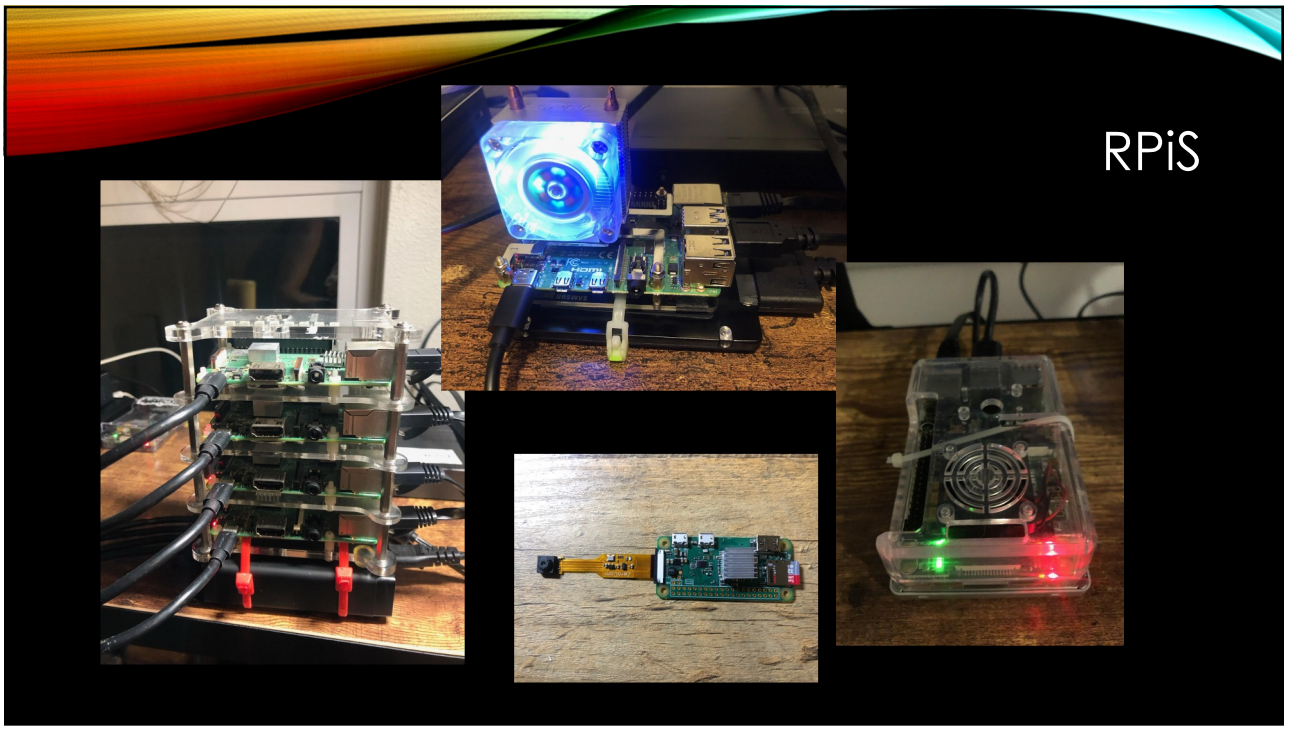
Your Lab!

- Virtualize
  - Proxmox - proxmox.com/en/
  - Virtualbox
  - UTM - https://github.com/utmapp/UTM
- PIs
- OpenWRT - https://openwrt.org/
- OpnSense - https://opnsense.org/

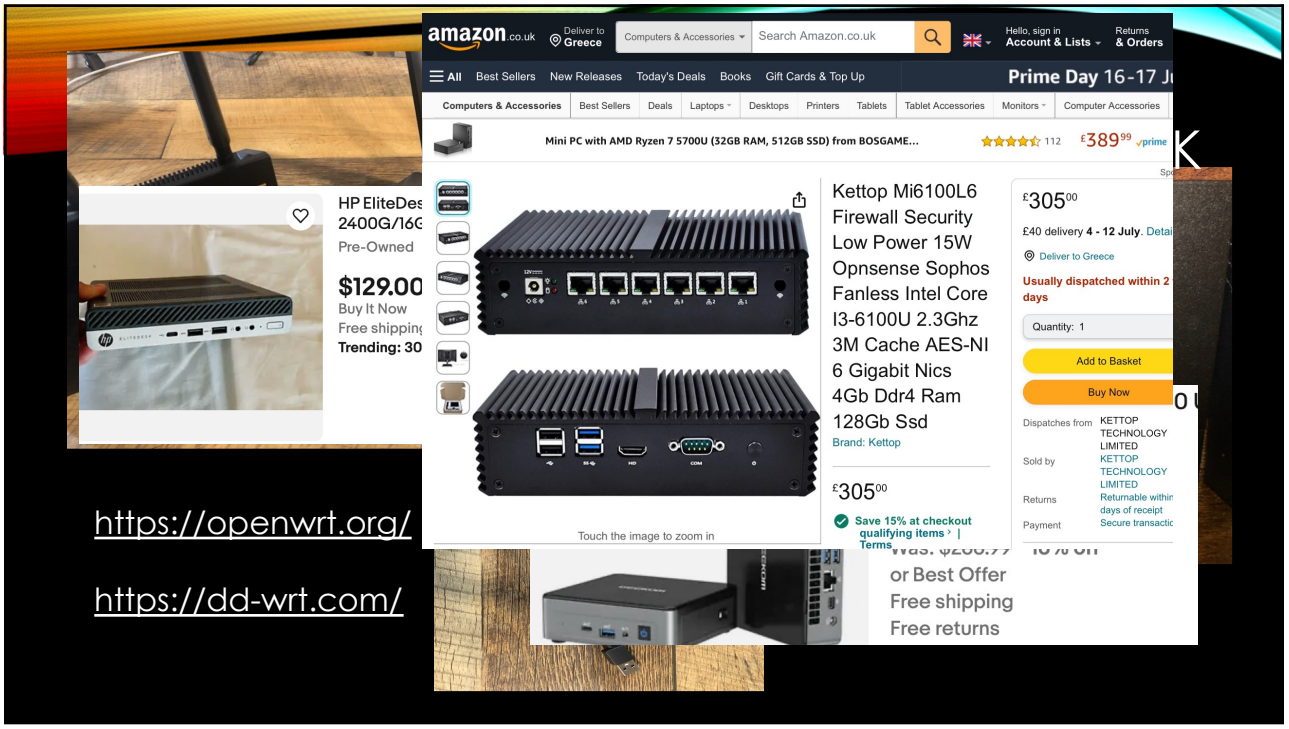
7


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
Guests
Running
Stopped
Resources
UTM
Start
Custom
Virtualize
Faster, but can only run the native CPU architecture.
Emulate
Slower, but can run other CPU architectures.
Existing
Open...
Download prebuilt from UTM Gallery...
Cancel
Storage
16%
of 4 CPU(s)
37%
11.69 GiB of 31.26 GiB
15%
135.87 GiB of 888.78 GiB

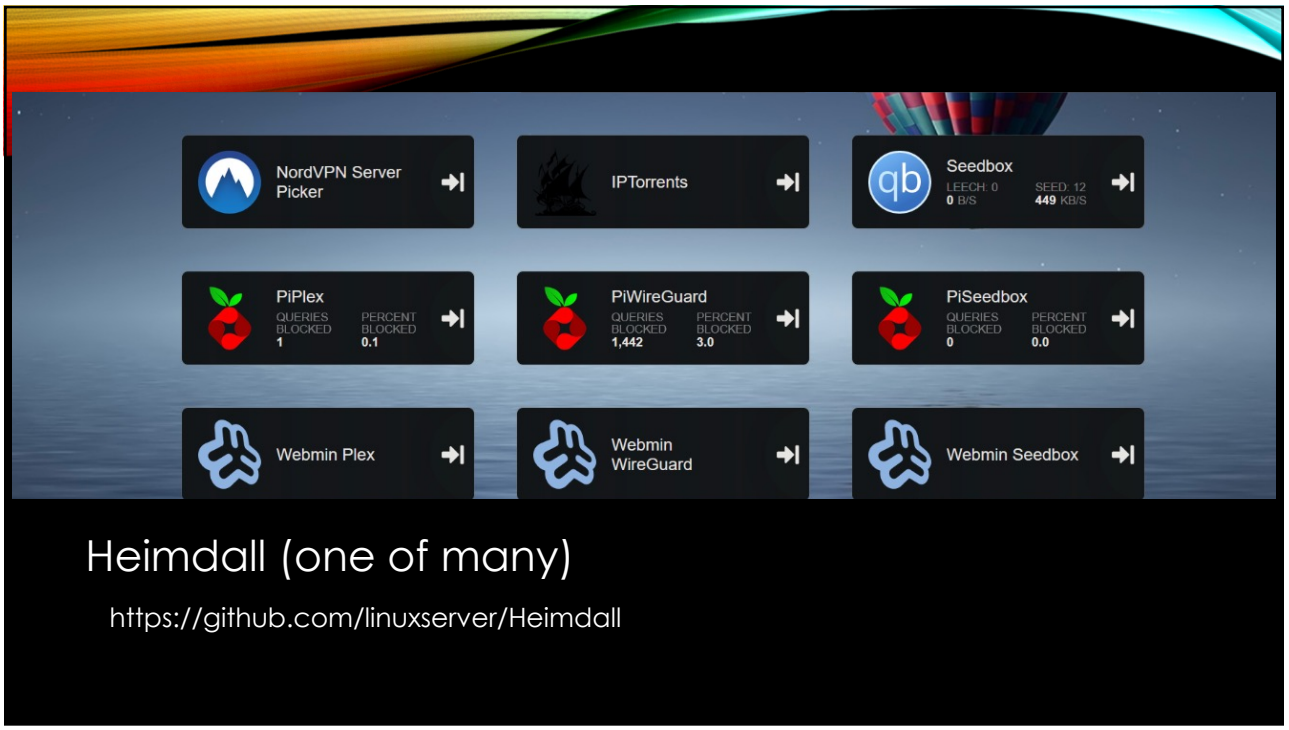
8


RPiS

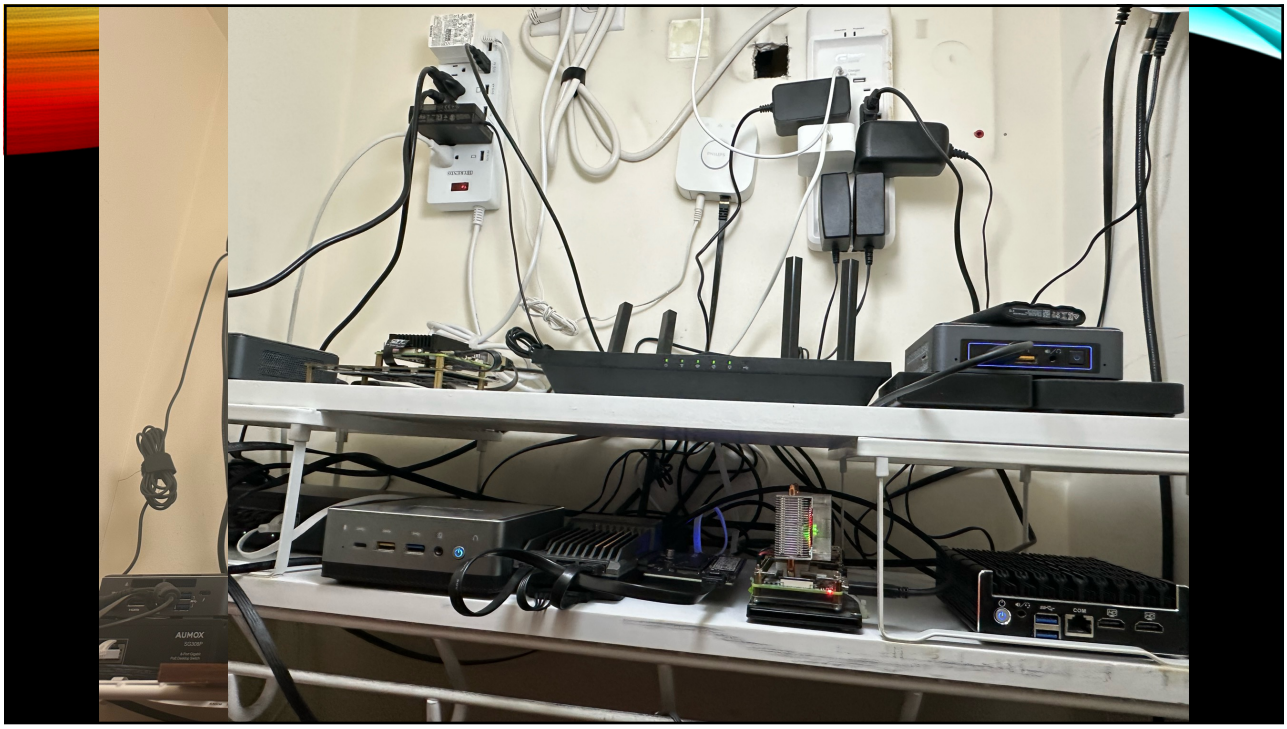
9


amazon.co.uk
Deliver to Greece
Search Amazon.co.uk
Hello, sign in Account & Lists
Returns & Orders
All Best Sellers New Releases Today's Deals Books Gift Cards & Top Up
Prime Day 16-17 J
Computers & Accessories Best Sellers Deals Laptops Desktops Printers Tablets Tablet Accessories Monitors Computer Accessories
Mini PC with AMD Ryzen 7 5700U (32GB RAM, 512GB SSD) from BOSGAME...
£389.99
Kettop Mi6100L6 Firewall Security Low Power 15W Opnsense Sophos Fanless Intel Core I3-6100U 2.3Ghz 3M Cache AES-NI 6 Gigabit Nics 4Gb Ddr4 Ram 128Gb Ssd
Brand: Kettop
£305.00
Touch the image to zoom in
£305.00
£40 delivery 4 - 12 July.
Deliver to Greece
Usually dispatched within 2 days
Quantity: 1
Add to Basket
Buy Now
Dispatches from KETTOP TECHNOLOGY LIMITED
Sold by KETTOP TECHNOLOGY LIMITED
Returns Returnable within days of receipt
Payment Secure transactic
Save 15% at checkout qualifying items | Terms
or Best Offer
Free shipping
Free returns
HP EliteDes
2400G/16G
Pre-Owned
$129.00
Buy It Now
Free shippin
Trending: 30
https://openwrt.org/
https://dd-wrt.com/

10


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

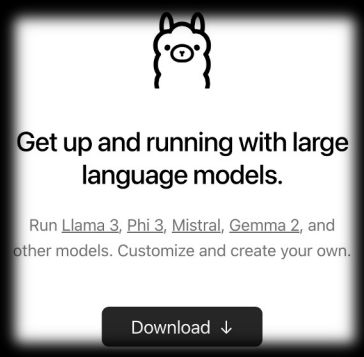
11



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!!! (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>  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
```

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 - 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

16

NOW WHAT PART 3

SPIRE
SPIFFE-based zero trust for microservices

- k3sup - https://github.com/alexellis/k3s
- Rancher - https://rancher.com/do

- HomePwn -

10 Ansible Tricks

Nikto Pentests

Trivy
Container and software security scanner

/installation/

/HomePWN

Google Tsunami Security Scanner

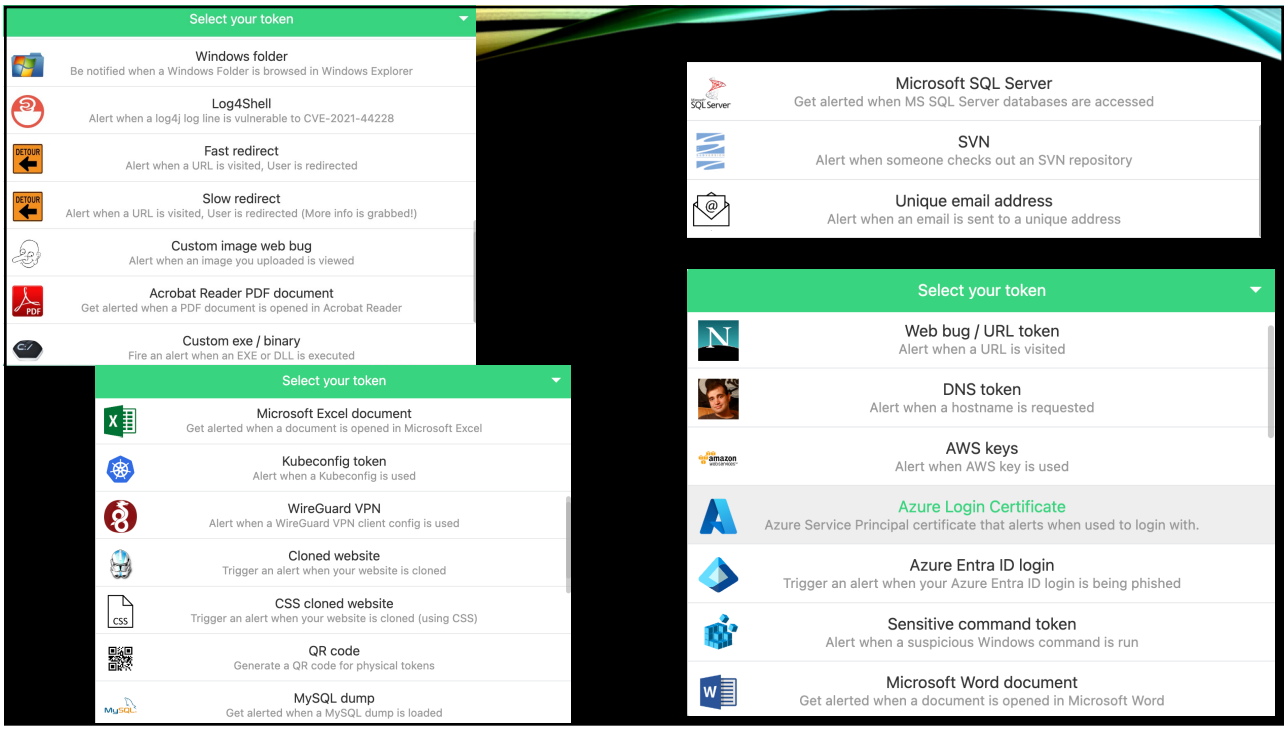
17

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

18



19

More Random Ideas

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)

20

ADHD

ADHD Version: **4.0.0** | GitHub Page | Project Page

Black Hills Information Security

ADHD

- Credentials
- Artillery
  - Example 1: Running Artillery
  - Example 2: Triggering a Honeyport
  - Example 3: Adding a File to a Watched Directory
- Bear Trap
  - Example 1: Basic Usage
- BeEF
  - Example 1: Hooking a Web Browser
  - Example 2: Browser Based Exploitation With BeEF
- CanaryTokens
  - Example 1: Creating Callbacks Using Local Canary Instance
  - Example 2: Creating Callbacks Using CanaryTokens.org
- Cowrie
  - Example 1: Running Cowrie
  - Example 2: Cowrie In Action
  - Example 3: Viewing Cowrie's Logs

21

MONITORING

wazuh.com


```
curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

22

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.

23

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.

24

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.

25

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

26

Thank You!

Kat Fitzgerald

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

evilkat@rnbwmail.com

27