DIY Cyber Mayhem:
A Quirky Dive into Homelabs & Honeypots

Kat Fitzgerald evilkat@rnbwmail.com

github.com/rnbwkat/presents

rnbwkat@infosec.exchange
rnbwkat.bsky.social

theunfrostedfiles.com
sashatheflamingo.xyz

youtube.com/@rnbwkatandtequila
(first episode being recorded soon)

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 We Aren't Here

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

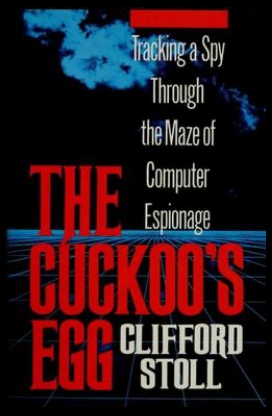
5

Why 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

The Rise of the Fancy Era



- *Throwback Thursday: When "The Cuckoo's Egg" was the hottest cybersecurity page-turner (~~$0.75~~ --> $2.13)*
- *The shift towards advanced, AI-driven, and automated security tools.*
- *The dangers of over reliance on these tools.*
- *Recent high-profile breaches: What went wrong?*

8

SOME BASICS

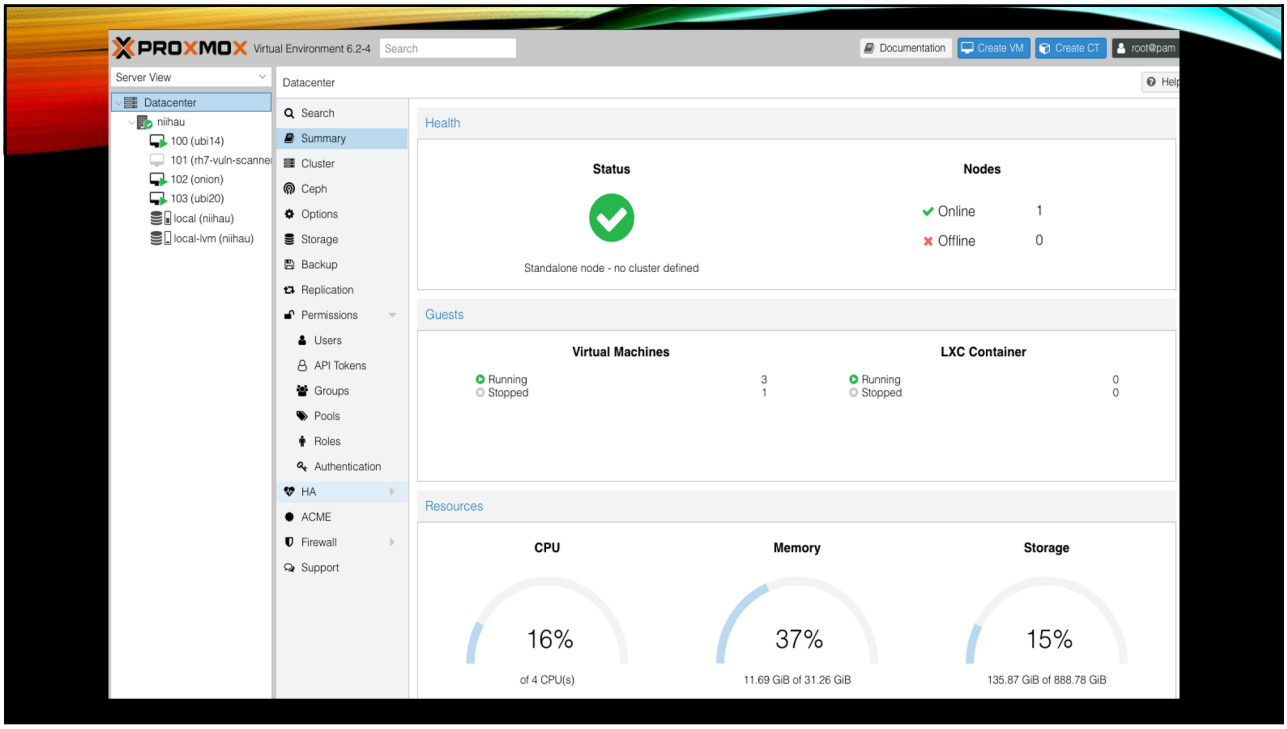
Your Lab!

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

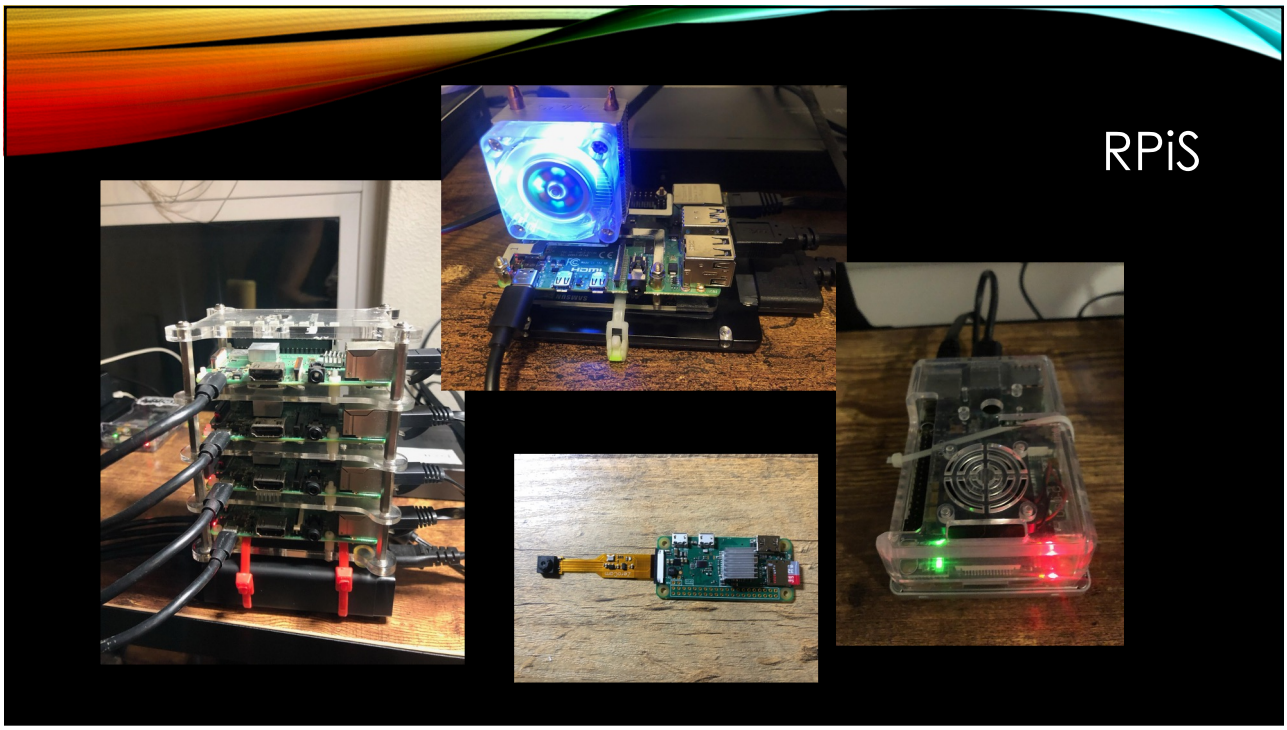
9

VIRTUALIZE!

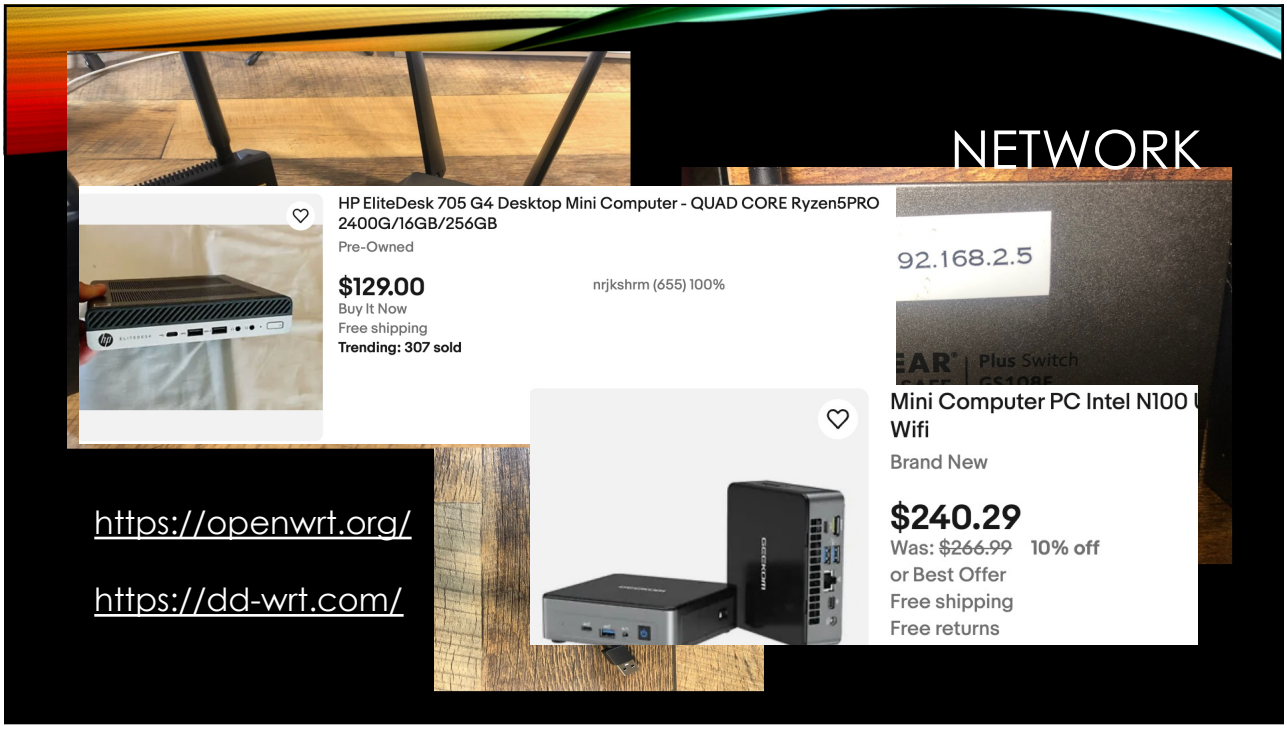
10


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

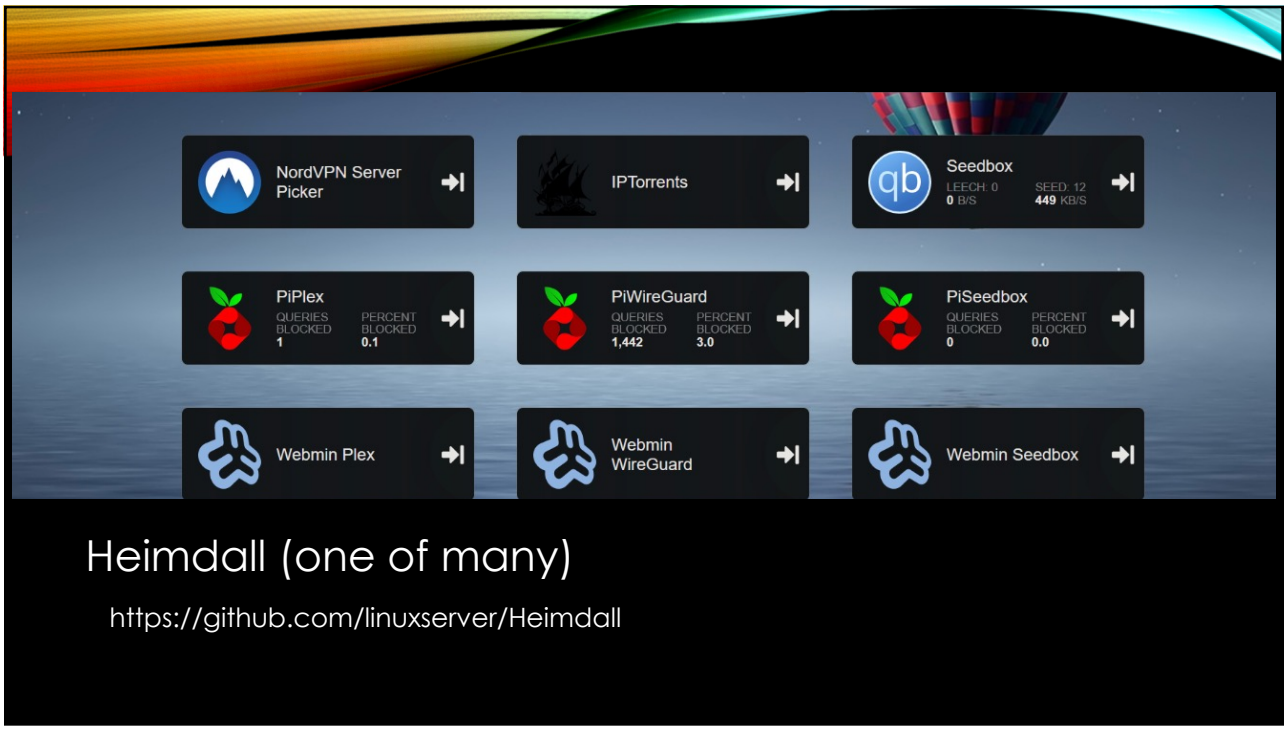
11


RPiS

12

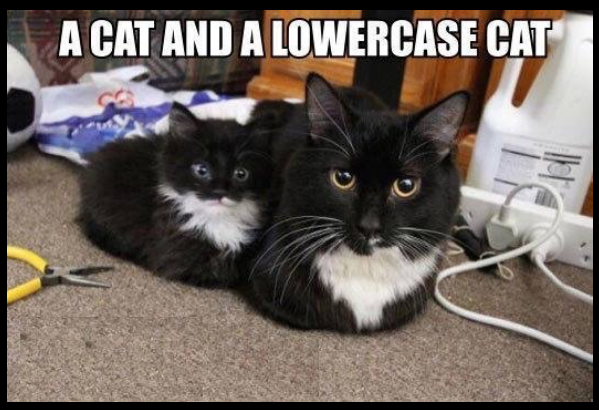

NETWORK
HP EliteDesk 705 G4 Desktop Mini Computer - QUAD CORE Ryzen5PRO 2400G/16GB/256GB
Pre-Owned
$129.00
Buy It Now
Free shipping
Trending: 307 sold
nrjkshrm (655) 100%
92.168.2.5
Mini Computer PC Intel N100
Wifi
Brand New
$240.29
Was: $266.99 10% off
or Best Offer
Free shipping
Free returns
https://openwrt.org/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

13


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

14

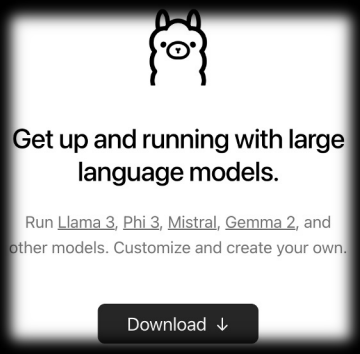
Proxmox Demo



16

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)



17

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.

18

A Quick Cluster - 5 minutes

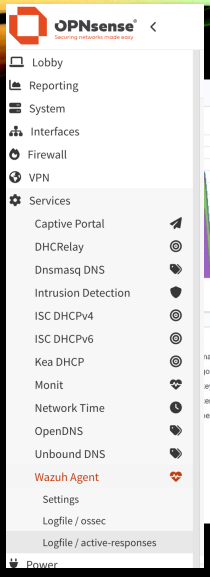
- 4 nodes
  - Raspberry Pi 3 Model B Plus Rev 1.3
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2

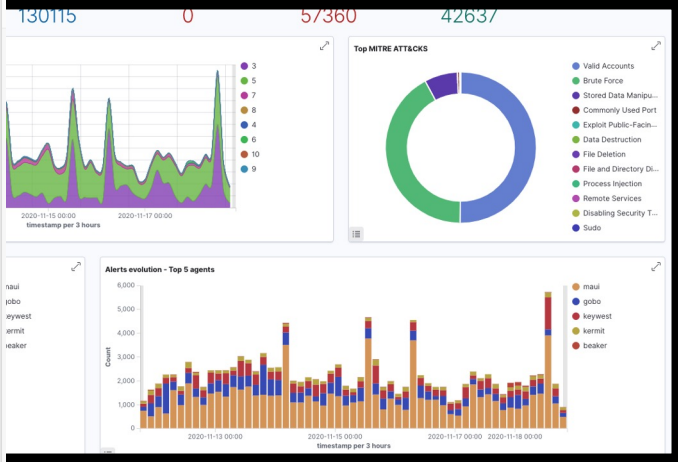
```
$ k3sup install --ip 192.168.2.70 --user pi --context isis --local-path $HOME/.kube/config --k3s-channel latest
$ export KUBECONFIG=/Users/kat8172/.kube/config

$ 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
```

19

MONITORING

wazuh.com






```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

21

Break It – Learn It

- VulnHub - www.vulnhub.com
- owasp.org/projects/
  - Learn secure coding - WebGoat owasp.org/www-project-webgoat
  - Practice modern AppSec attacks - Juice Shop owasp.org/www-project-juice-shop
  - Master recon & mapping - Amass owasp.org/www-project-amass
- SDR!! - github.com/luigifcruz/pisdr-image

22

Juice Shop

- What is Juice Shop?
  - OWASP Juice Shop is a deliberately insecure web application used for training, security demos, and CTF-style hacking challenges. It simulates a vulnerable e-commerce site and includes real-world OWASP Top 10 flaws
- Install Docker: https://docs.docker.com/get-docker/
- Open a terminal and run:

```
docker run --rm -p 3000:3000 bkimminich/juice-shop
```

- Open your browser and go to:
  http://localhost:3000

23

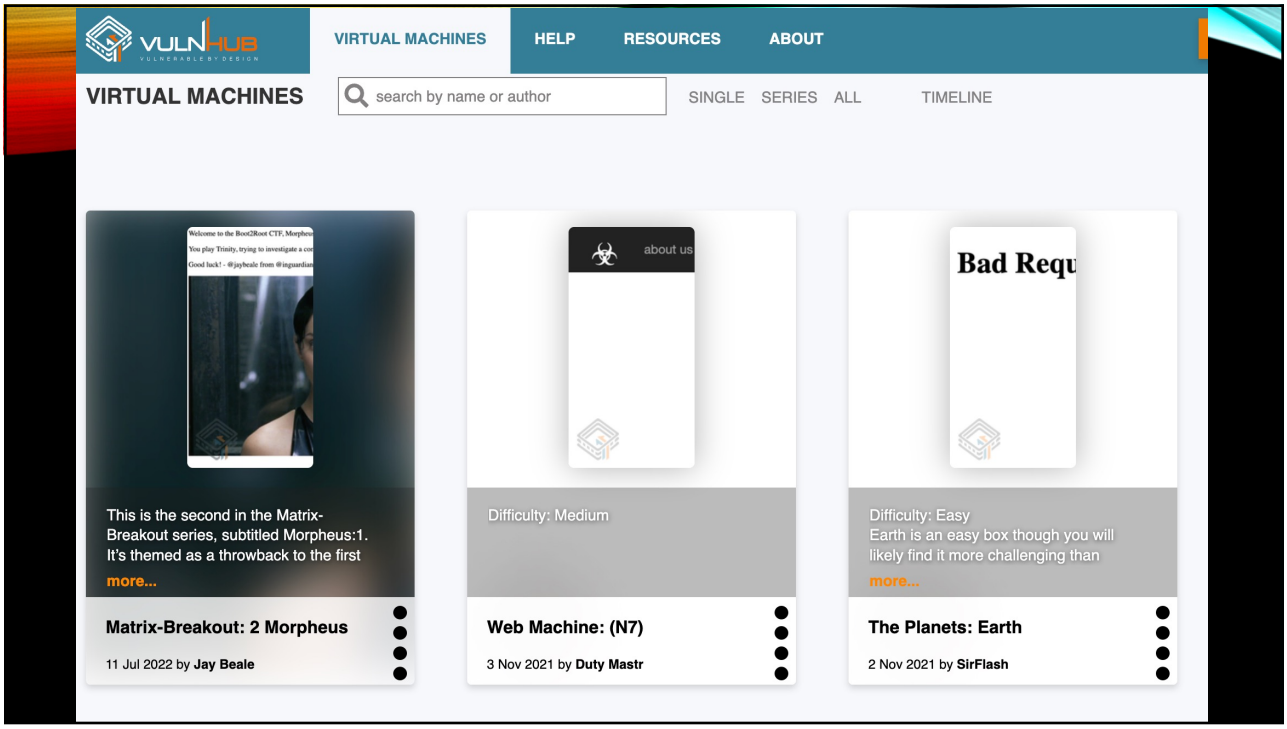
Challenges to Try

- Log in as admin (check source code and hints)
- Exploit the "Forgot Password" flow
- Perform XSS in the search box
- Mess with the product review form
- Access unauthorized account pages

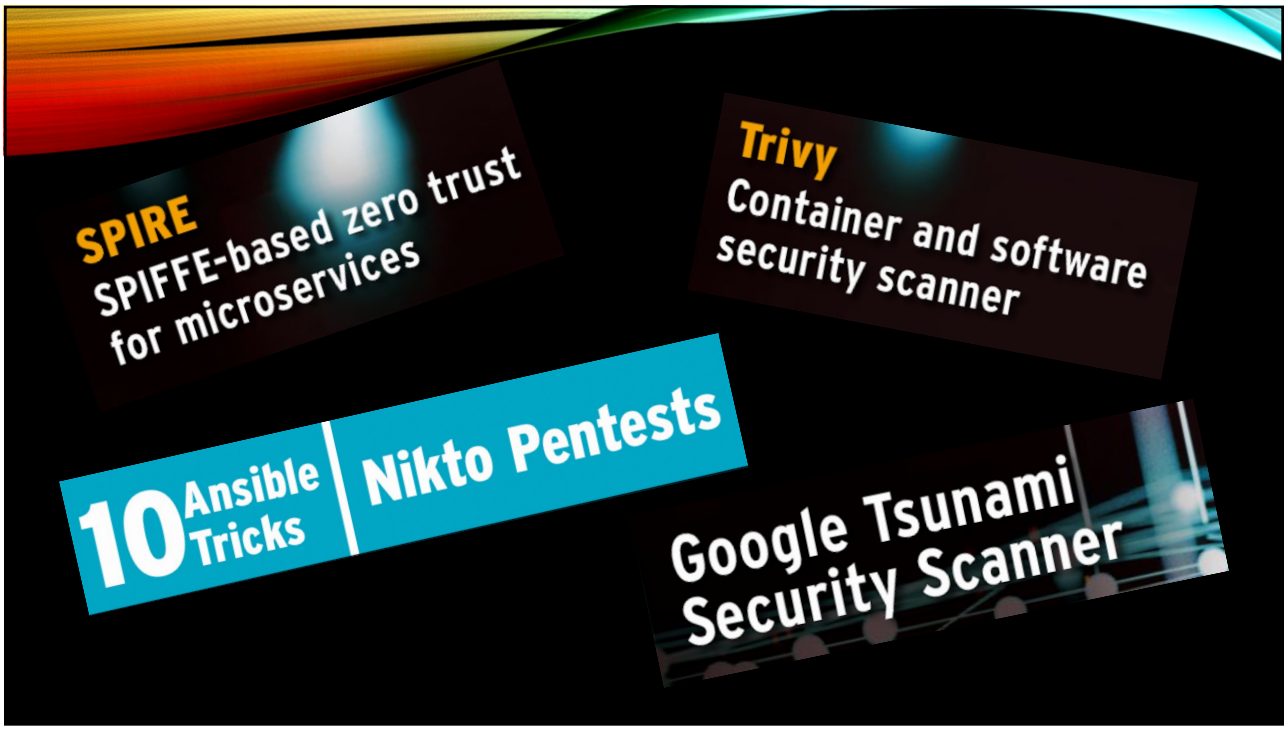
Suricata, OpenCanary, or Wazuh to capture logs of simulated attacks

Try using an LLM like LLaMA or GPT to summarize Suricata logs and find patterns in attacker behavior

24


VULNHUB
VULNERABLE BY DESIGN
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
VIRTUAL MACHINES
search by name or author
SINGLE
SERIES
ALL
TIMELINE
This is the second in the Matrix-Breakout series, subtitled Morpheus:1. It's themed as a throwback to the first
more...
Matrix-Breakout: 2 Morpheus
11 Jul 2022 by Jay Beale
about us
Difficulty: Medium
Web Machine: (N7)
3 Nov 2021 by Duty Mastr
Bad Requ
Difficulty: Easy
Earth is an easy box though you will likely find it more challenging than
more...
The Planets: Earth
2 Nov 2021 by SirFlash

25


SPIRE
SPIFFE-based zero trust for microservices
Trivy
Container and software security scanner
10 Ansible Tricks
Nikto Pentests
Google Tsunami Security Scanner

26

Homelab AI Node – 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

27

Picture Time!

- nextcloud.com – It just works!
- Tenable - tenable.com/products/nessus/nessus-essentials
- pwnagotchi.ai - Pi Zero! (dated, but still works!)
- homelabos.com – All-In-One
- Flare VM - github.com/mandiant/flare-vm
  - Windows malware-analysis & reverse-engineering VM
- CloudGoat - github.com/rhinosecuritylabs/cloudgoat
  - "vulnerable by design" cloud lab for IAM / S3 misconfig
- Kubernetes Goat- madhuakula.com/kubernetes-goat/docs
  - Kubernetes mis-configurations and attack/defence lab

28

OODA vs CCAD

- OODA
  - Observe
  - Orient
  - Decide
  - Act
- CCAD
  - Confuse
  - Confound
  - Annoy
  - Delay

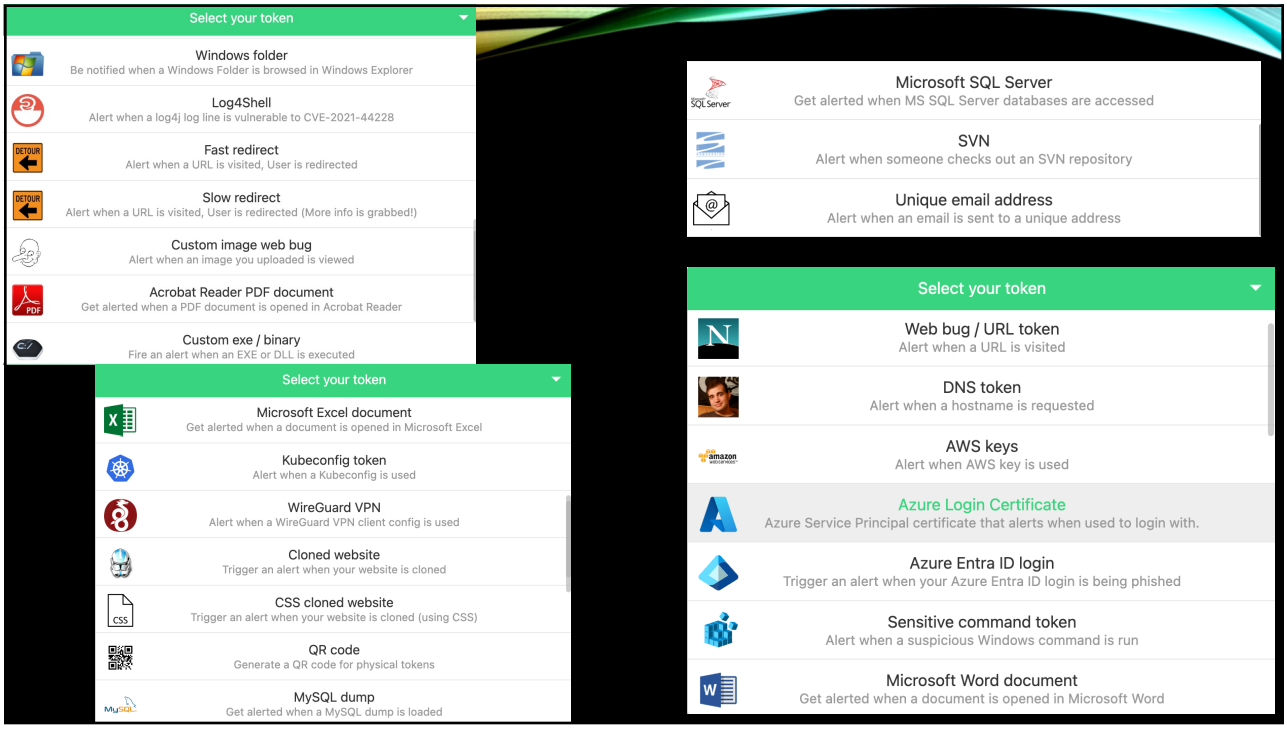
29

HONEYPOTS!

- OpenCanary -- opencanary.readthedocs.io/en/latest/
- Honey Badger -- github.com/adhdproject/honeybadger (GEO!)
- Community Honey Network -- communityhoneynetwork.readthedocs.io/en/stable/
- 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

30


Select your token
Windows folder
Be notified when a Windows Folder is browsed in Windows Explorer
Log4Shell
Alert when a log4j log line is vulnerable to CVE-2021-44228
Fast redirect
Alert when a URL is visited, User is redirected
Slow redirect
Alert when a URL is visited, User is redirected (More info is grabbed!)
Custom image web bug
Alert when an image you uploaded is viewed
Acrobat Reader PDF document
Get alerted when a PDF document is opened in Acrobat Reader
Custom exe / binary
Fire an alert when an EXE or DLL is executed
Select your token
Microsoft Excel document
Get alerted when a document is opened in Microsoft Excel
Kubeconfig token
Alert when a Kubeconfig is used
WireGuard VPN
Alert when a WireGuard VPN client config is used
Cloned website
Trigger an alert when your website is cloned
CSS cloned website
Trigger an alert when your website is cloned (using CSS)
QR code
Generate a QR code for physical tokens
MySQL dump
Get alerted when a MySQL dump is loaded
Microsoft SQL Server
Get alerted when MS SQL Server databases are accessed
SVN
Alert when someone checks out an SVN repository
Unique email address
Alert when an email is sent to a unique address
Select your token
Web bug / URL token
Alert when a URL is visited
DNS token
Alert when a hostname is requested
AWS keys
Alert when AWS key is used
Azure Login Certificate
Azure Service Principal certificate that alerts when used to login with.
Azure Entra ID login
Trigger an alert when your Azure Entra ID login is being phished
Sensitive command token
Alert when a suspicious Windows command is run
Microsoft Word document
Get alerted when a document is opened in Microsoft Word

31


my Honeypot Empire
Started as a weekend project in 2018
Now spans 5 continents, 17 countries
Ukraine
Don't underestimate honeypots in quieter countries - (Luxembourg?)
Over 1.2 million attempted intrusions logged (as of 2024)
Deployment environments:
ISP networks
Cloud providers
University networks
Industrial control system simulations

32

Evolution

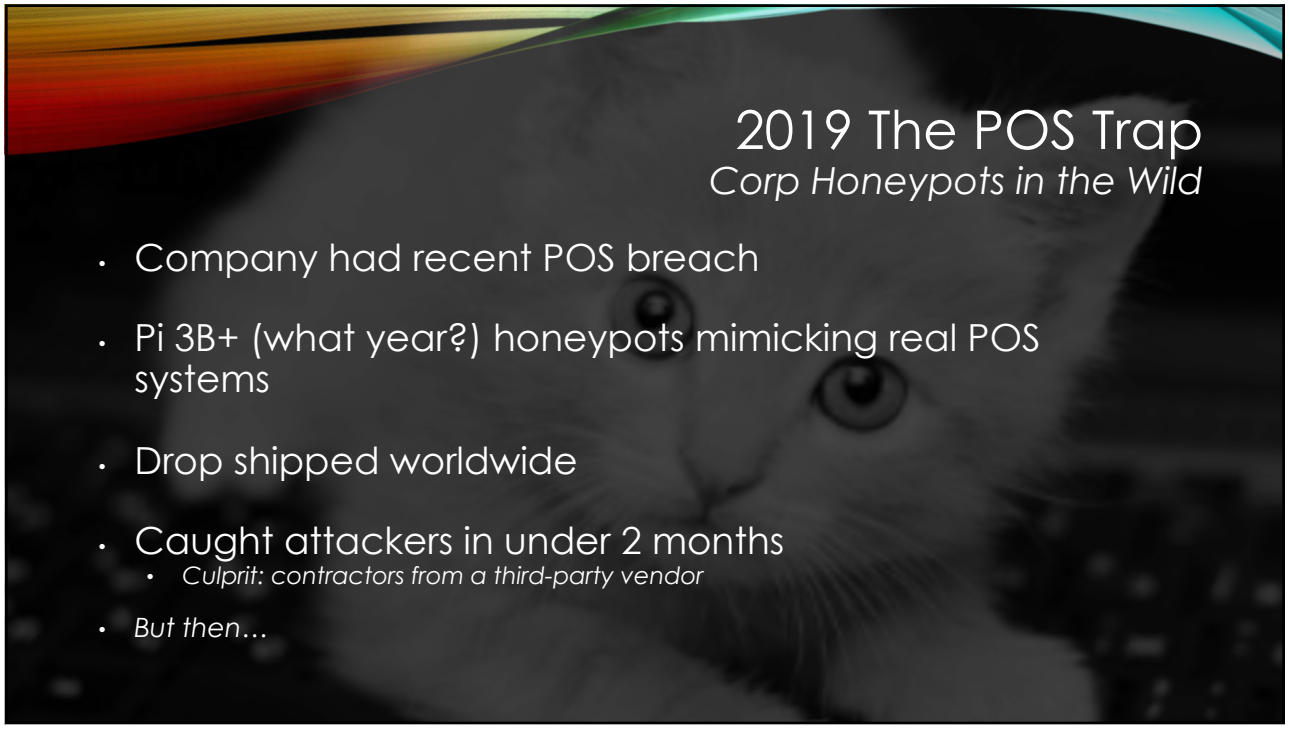
- 2018: Basic SSH and web honeypots (2018)
  - *Rebooted with nmap –f (and others)*
- 2020: Integrated deception networks w/breadcrumbs between systems
- 2021: HoneyTokens + IoT + Devices (Medical?)
- 2023: Added fake company environment with believable data
  - This was hard! What was I thinking?
  - *Bonus: Sasha helps write bios*
  - *New talk on the way!*
- 2024: Machine learning for dynamic response and adaptation (2024-25)
  - Current "Linux" agent

33

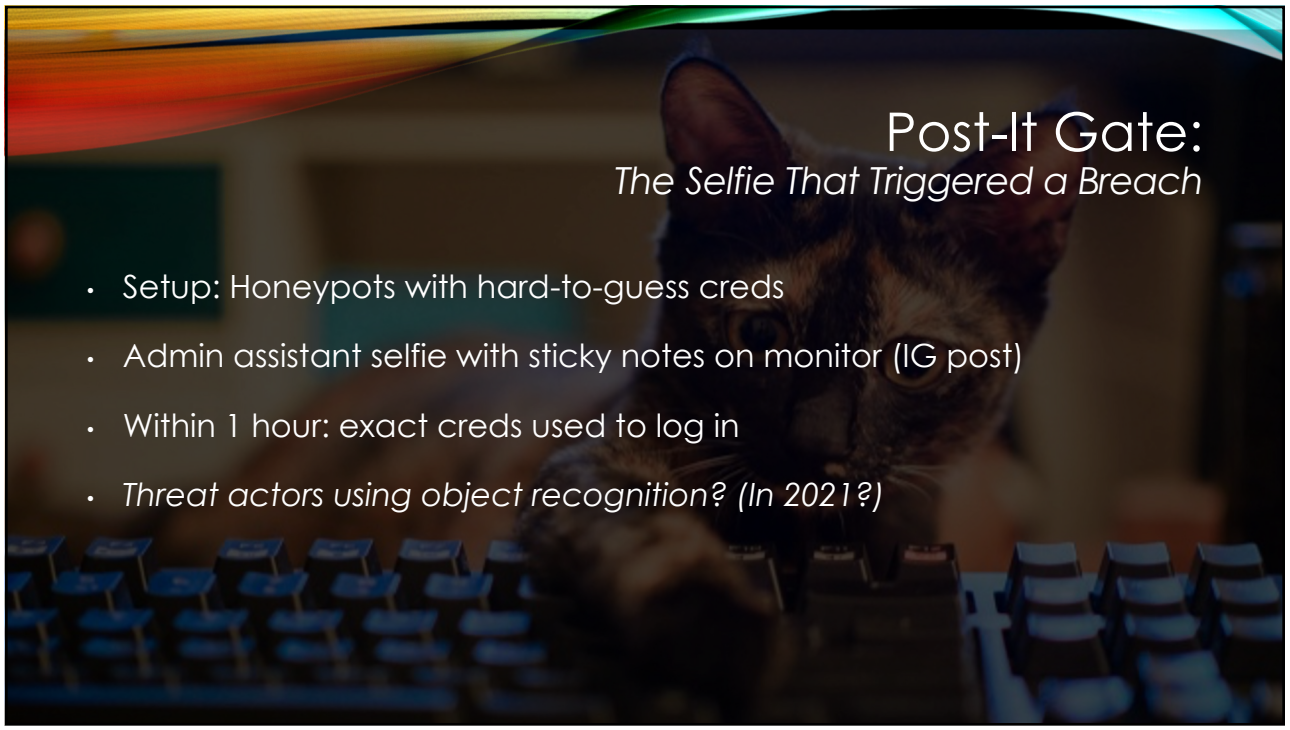
The Usual Suspects (Types of Attacks)

- SSH Brute Force Attacks: Highest in Ukraine (12,000 attempts in a month!)
- IoT Malware: Brazil had a field day with malware 9,600 infection attempts
- RDP Exploits: USA leading in RDP-based attacks
- Web Exploits: Japan had some sneaky XSS attempts
- *Fun fact: One botnet consistently tries to log in as "admin" with the password "123456"—everywhere. Global mediocrity at its finest.*

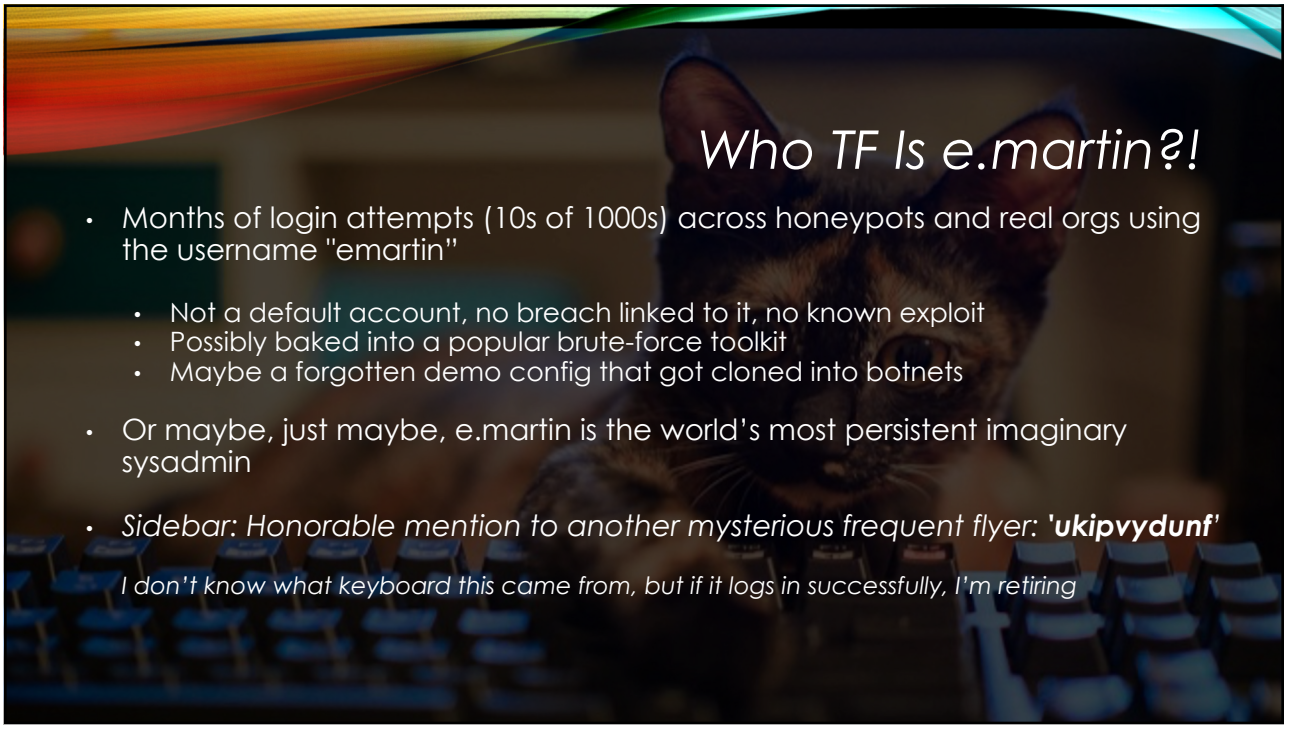
34


2019 The POS Trap
Corp Honeypots in the Wild
• Company had recent POS breach
• Pi 3B+ (what year?) honeypots mimicking real POS systems
• Drop shipped worldwide
• Caught attackers in under 2 months
• Culprit: contractors from a third-party vendor
• But then…

35


Post-It Gate:
The Selfie That Triggered a Breach
• Setup: Honeypots with hard-to-guess creds
• Admin assistant selfie with sticky notes on monitor (IG post)
• Within 1 hour: exact creds used to log in
• Threat actors using object recognition? (In 2021?)

36


Who TF Is e.martin?!
• Months of login attempts (10s of 1000s) across honeypots and real orgs using the username "emartin"
• Not a default account, no breach linked to it, no known exploit
• Possibly baked into a popular brute-force toolkit
• Maybe a forgotten demo config that got cloned into botnets
• Or maybe, just maybe, e.martin is the world's most persistent imaginary sysadmin
• *Sidebar: Honorable mention to another mysterious frequent flyer:* ***'ukipvydunf'***
I don't know what keyboard this came from, but if it logs in successfully, I'm retiring

37


Weird Attackers
• Messages left:
• "Try harder."
• "If this is a real company, just hire me."
• "I fixed your SSH config. You're welcome."

38

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.

39

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.

40

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.

41

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.

42

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!*

43

KEY TAKEAWAYS

- It's Playtime!
  - The beauty of virtualization
  - Don't forget about containers/proxmox
- Start small / build on it
  - Break it – build it – break it again
  - No right or wrong

github.com/awesome-selfhosted/awesome-selfhosted
github.com/paralax/awesome-honeypots

44

Technical Findings & Lessons Learned

- Password spray attacks still rule – but quality is declining
- Most attackers spend ~37 minutes before moving on *(but they return)*
- 72% attempt to disable logging as a first move
- Geographic coordination reveals professional infrastructure management
  - Same operations rotate between countries (Singapore → Germany → Lithuania → France)
- Advanced techniques coexist with amateur execution:
  - Plugin CVEs, directory traversal, XSS, LFI attacks
  - *But also: "Page not found" and lots of broken usernames*
- Threat landscape changes
  - From basic credential stuffing to advanced CVE exploitation

But seriously – why do we need to worry about AI?

45

Thank You!

Kat Fitzgerald

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

evilkat@rnbwmail.com

sashatheflamingo.xyz

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

46