FOLLOW THE COBWEBS

The Road ~~Less~~ Infosec Traveled

1

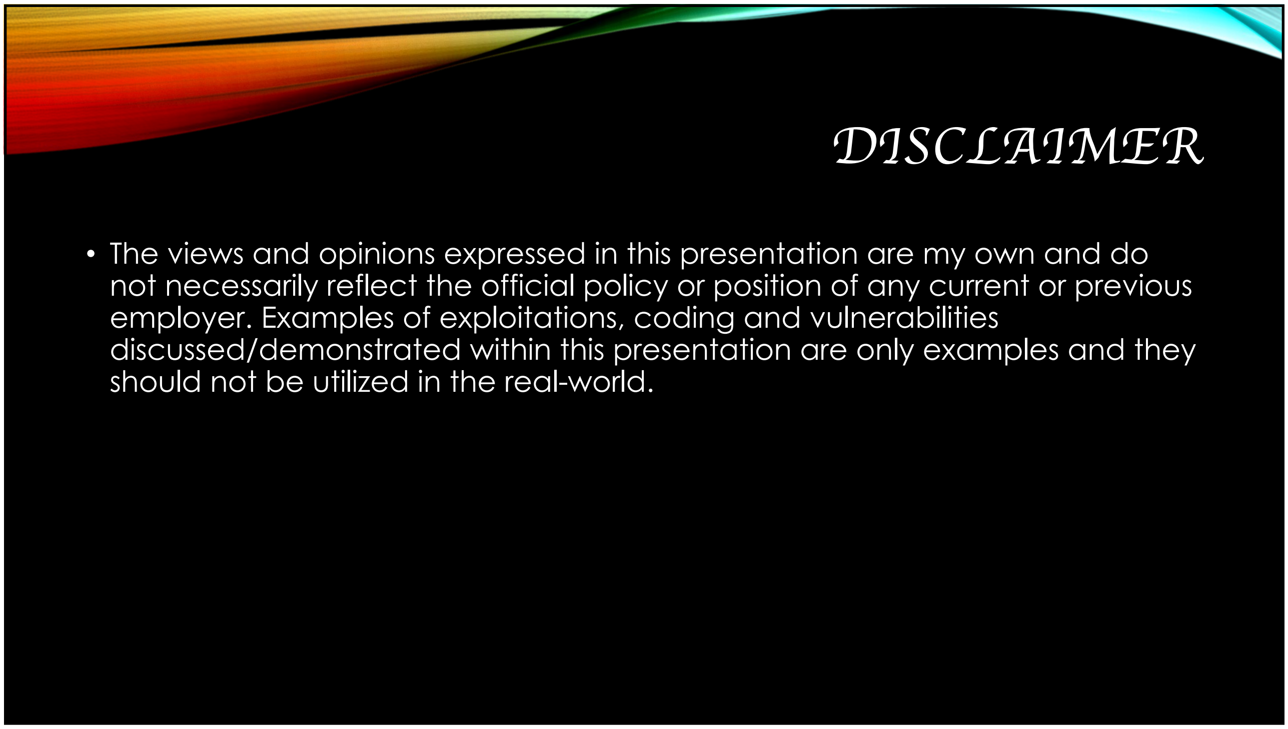
WHOAMI

$ whoami

Kat Fitzgerald (@rnbwkat or evilkat@rnbwmail.com)

- *Lead for BSidesChicago, CFP Lead BSidesPGH, Board Member Security BSides*
- *My first DEFCON was DC 3 (1995) with 16 speakers.*
- *Over 35(?) years in the Security field, focusing on building strong security teams and strong security infrastructures with an emphasis on Security Operations, Incident Response and Purple Teams.*
- *Based in Chicago and a natural creature of winter, you can typically find me sipping Casa Noble Anejo whilst simultaneously defending my networks using OSS, magic spells and Unicorns against a barrage of attackers.*
- *Photographer (it will make sense, I promise)*

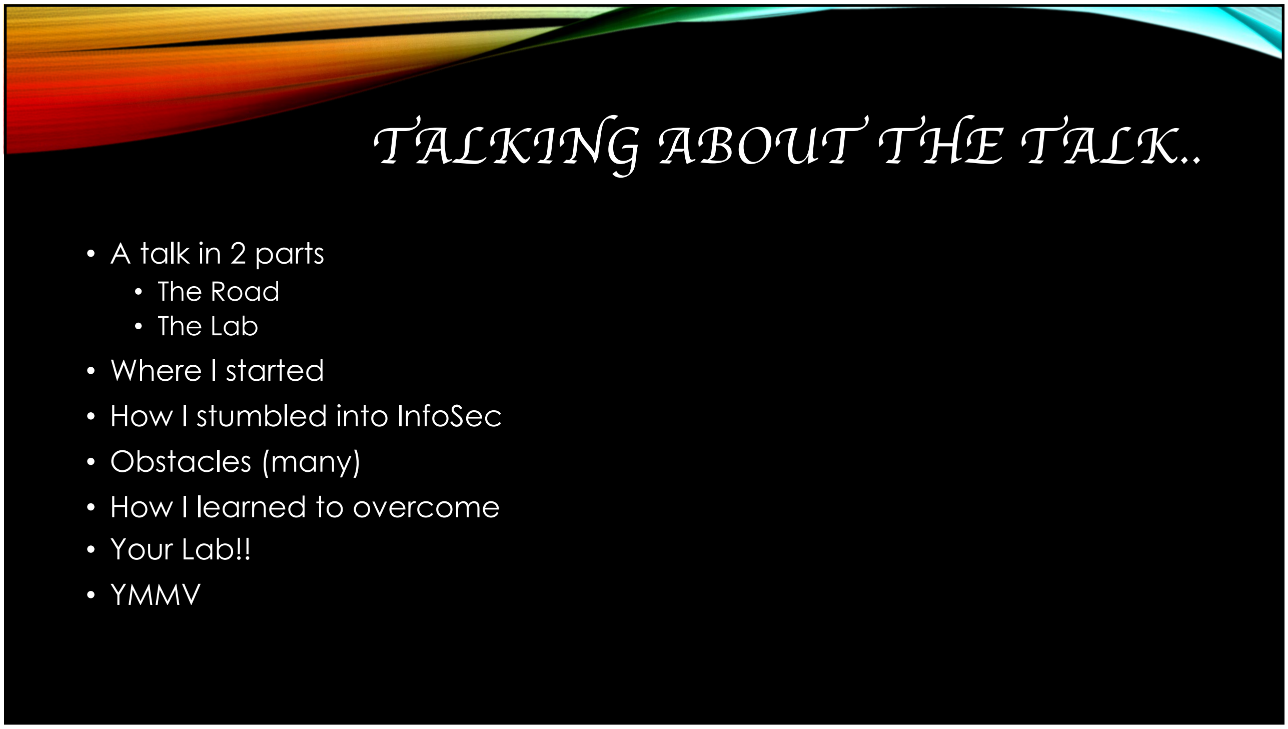
2



DISCLAIMER

- The views and opinions expressed in this presentation are my own and do not necessarily reflect the official policy or position of any current or previous employer. Examples of exploitations, coding and vulnerabilities discussed/demonstrated within this presentation are only examples and they should not be utilized in the real-world.

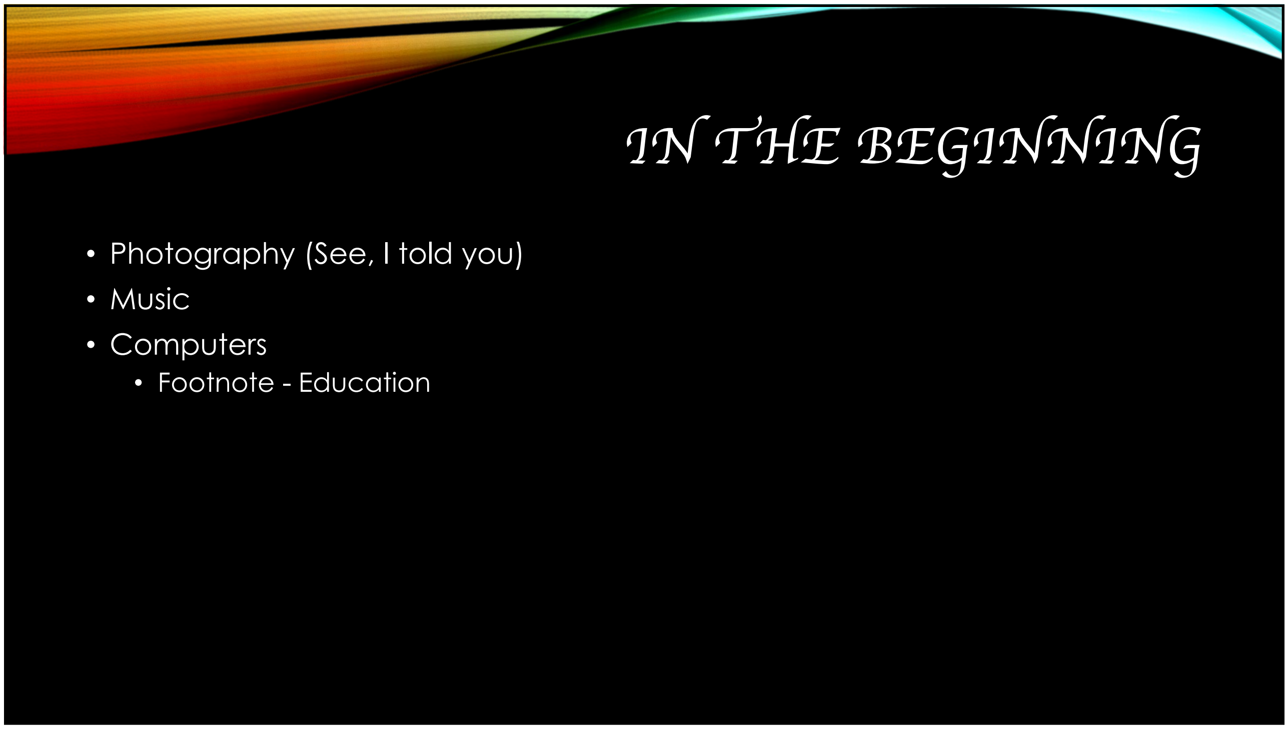
3



TALKING ABOUT THE TALK..

- A talk in 2 parts
  - The Road
  - The Lab
- Where I started
- How I stumbled into InfoSec
- Obstacles (many)
- How I learned to overcome
- Your Lab!!
- YMMV

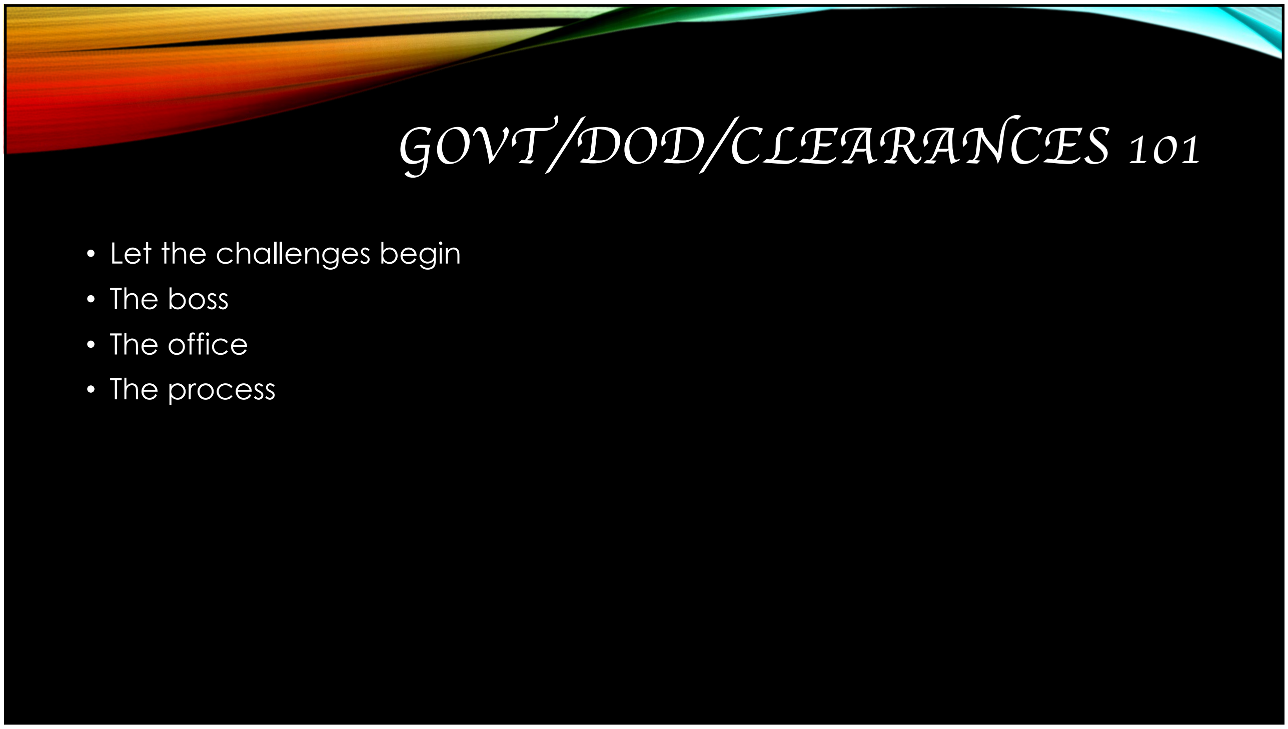
4



IN THE BEGINNING

- Photography (See, I told you)
- Music
- Computers
  - Footnote - Education

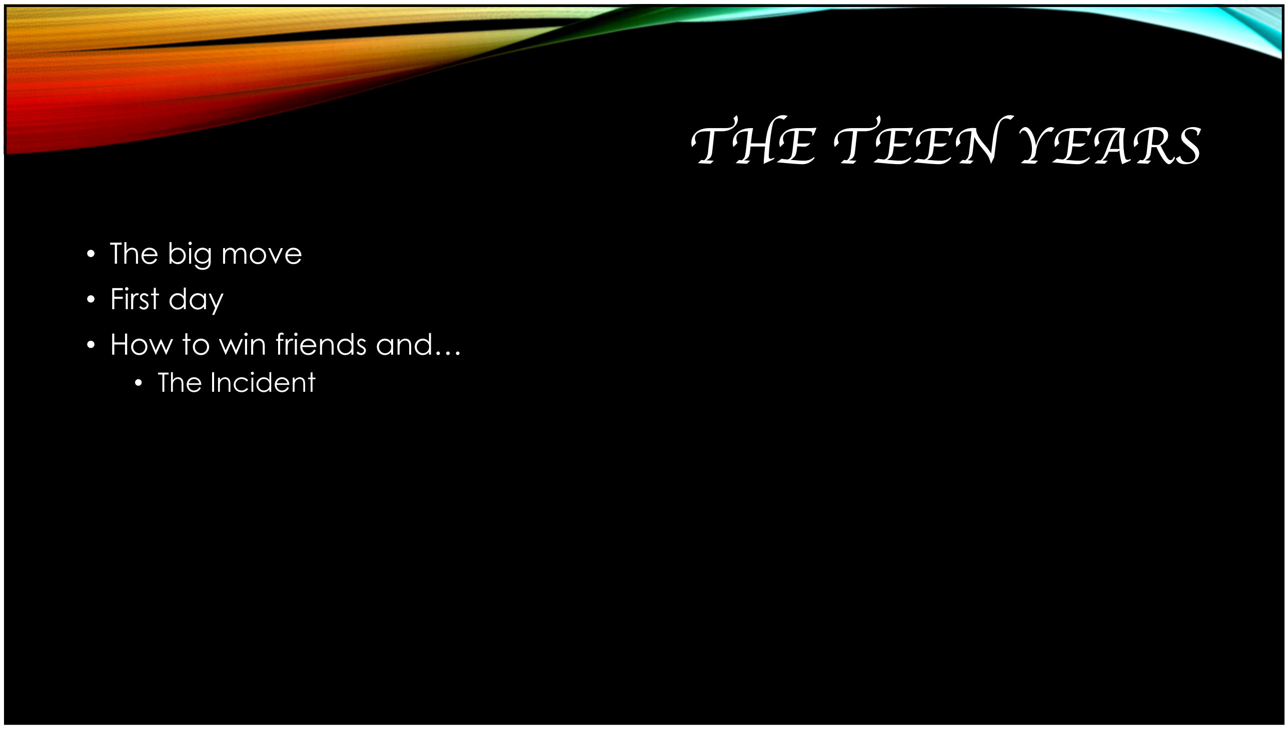
5



GOVT/DOD/CLEARANCES 101

- Let the challenges begin
- The boss
- The office
- The process

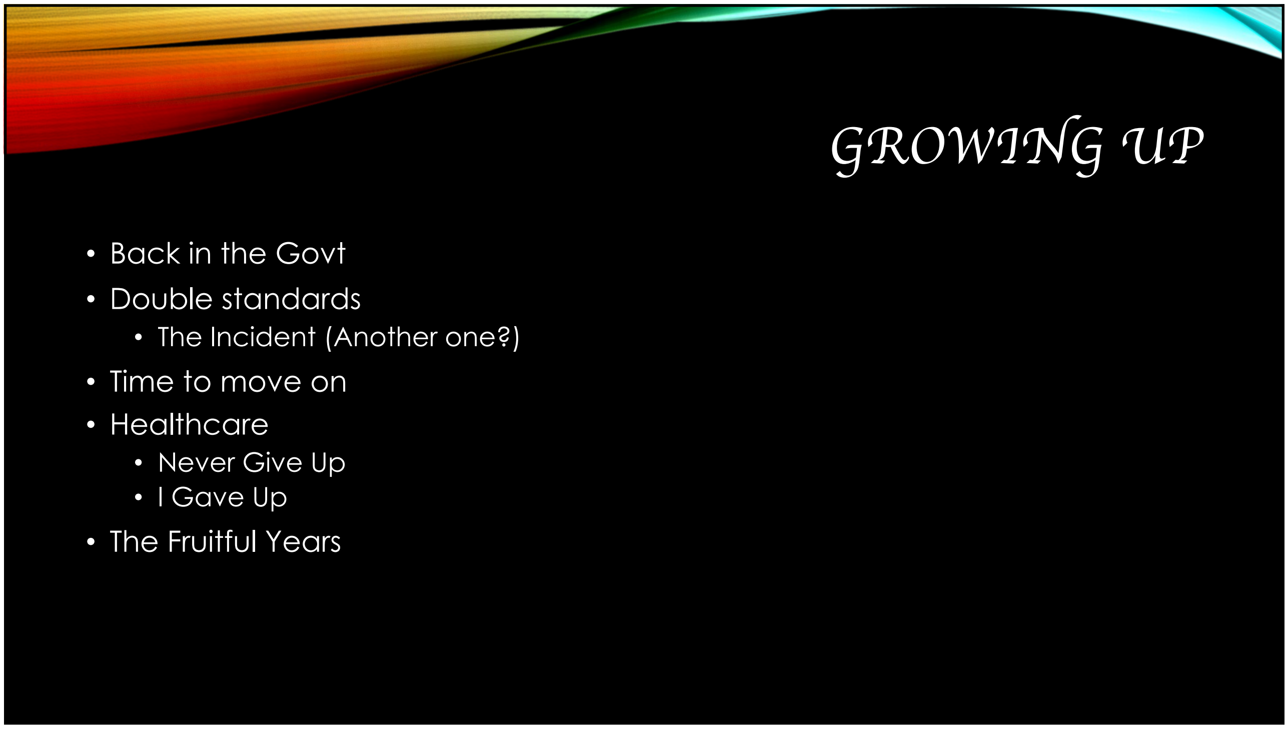
6



THE TEEN YEARS

- The big move
- First day
- How to win friends and…
  - The Incident

7



GROWING UP

- Back in the Govt
- Double standards
  - The Incident (Another one?)
- Time to move on
- Healthcare
  - Never Give Up
  - I Gave Up
- The Fruitful Years

8

BOSSES(?)

- Friends
  - Not always, everyone is human

9

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

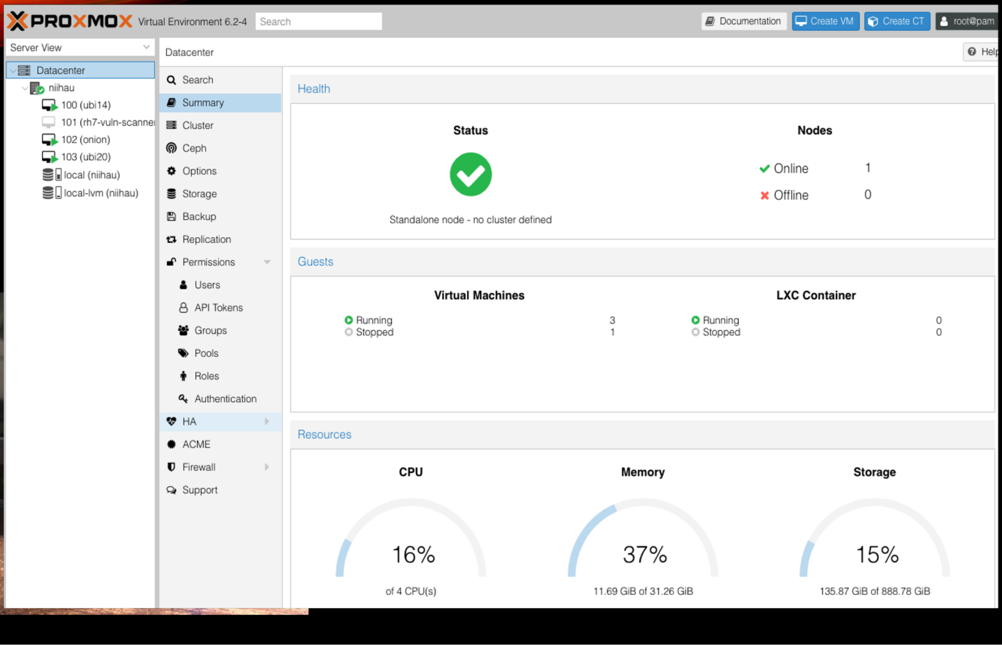
10

SOME BASICS

Your Lab!

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

11



Health

Status

Standalone node - no cluster defined

Nodes

✓ Online 1

✗ Offline 0

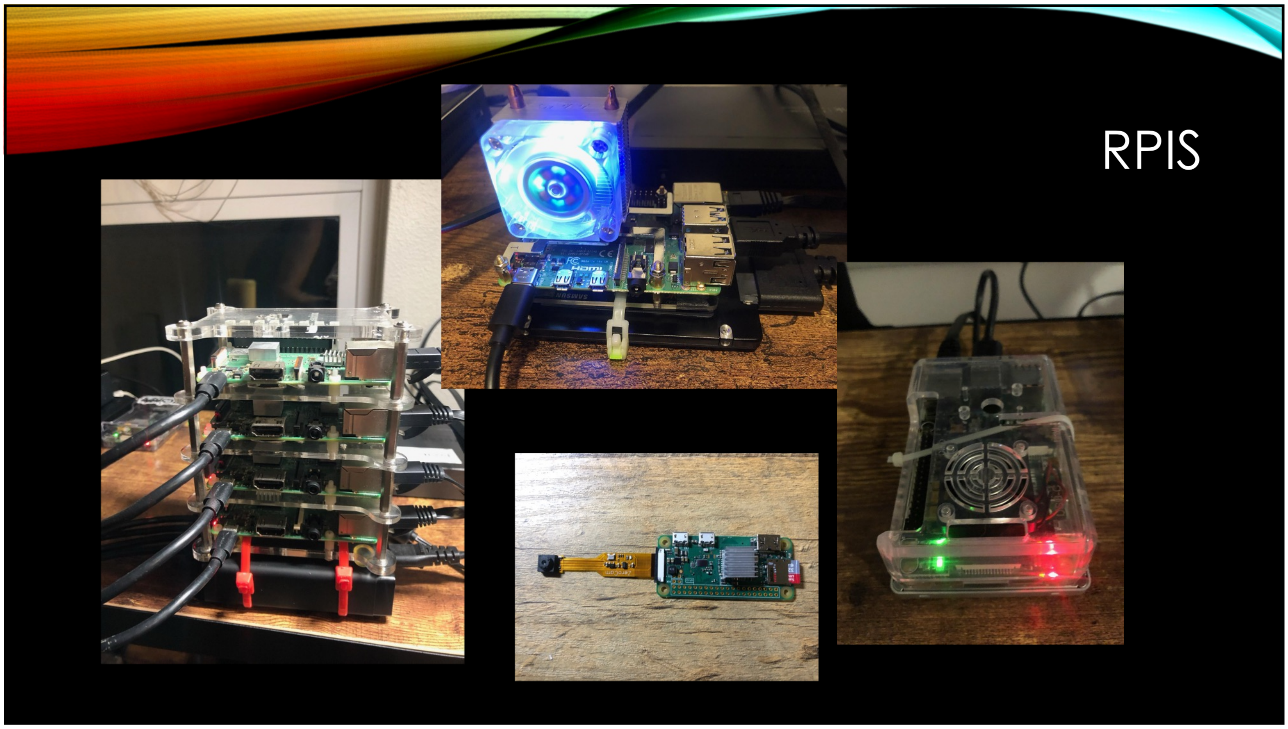
Guests

Virtual Machines		LXC Container	
Running	3	Running	0
Stopped	1	Stopped	0

Resources

CPU	Memory	Storage
16%	37%	15%
of 4 CPU(s)	11.69 GiB of 31.26 GiB	135.87 GiB of 888.78 GiB

12



RPIS

13

NETWORK

14

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)
- Wazuh (more in a minute)

15

A QUICK CLUSTER - 5 MINUTES

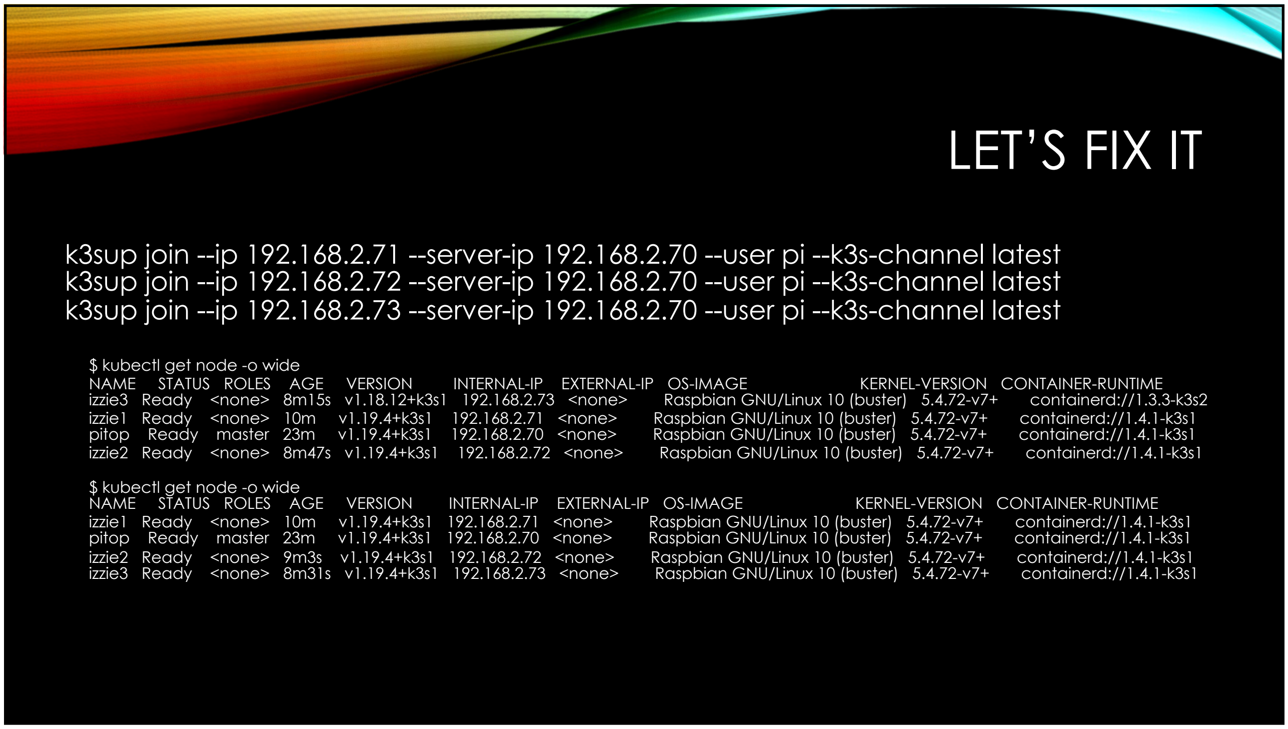
- 4 nodes
  - Raspberry Pi 3 Model B Plus Rev 1.3
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2
  - Raspberry Pi 3 Model B Rev 1.2

```
$ 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>   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
```

16



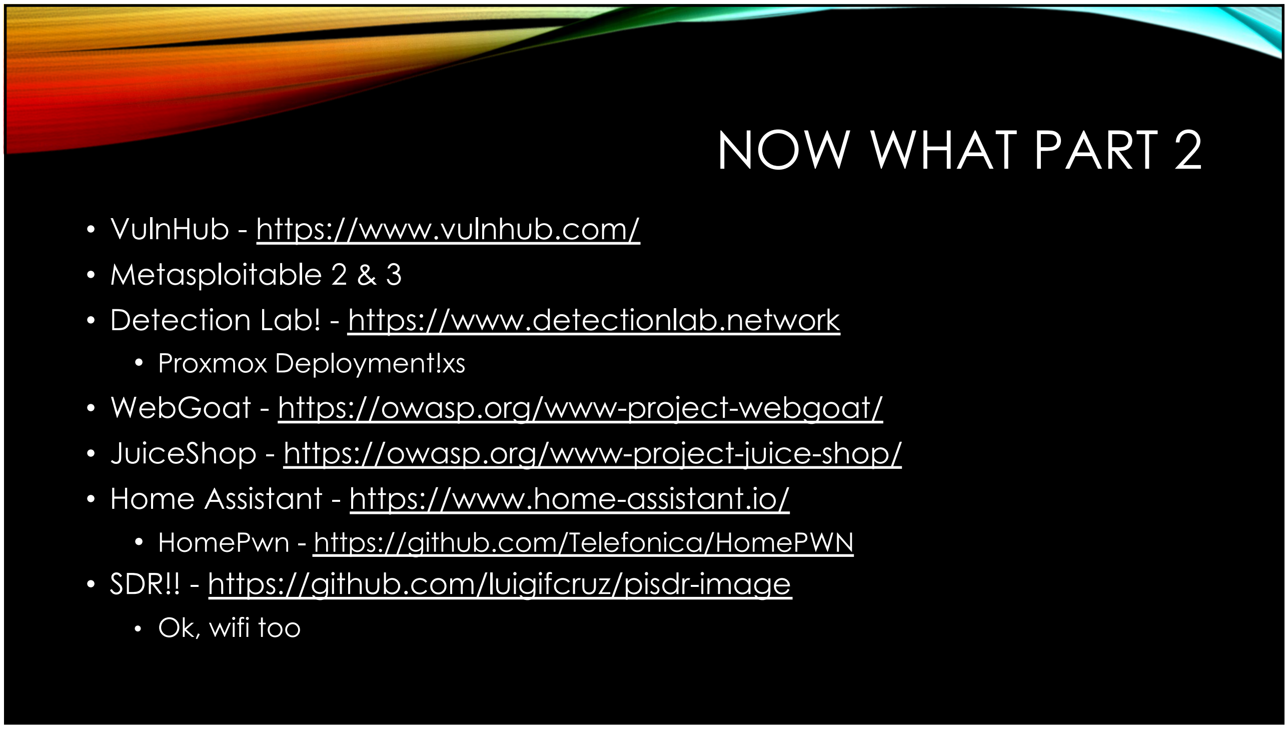
LET’S FIX IT

```
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
```

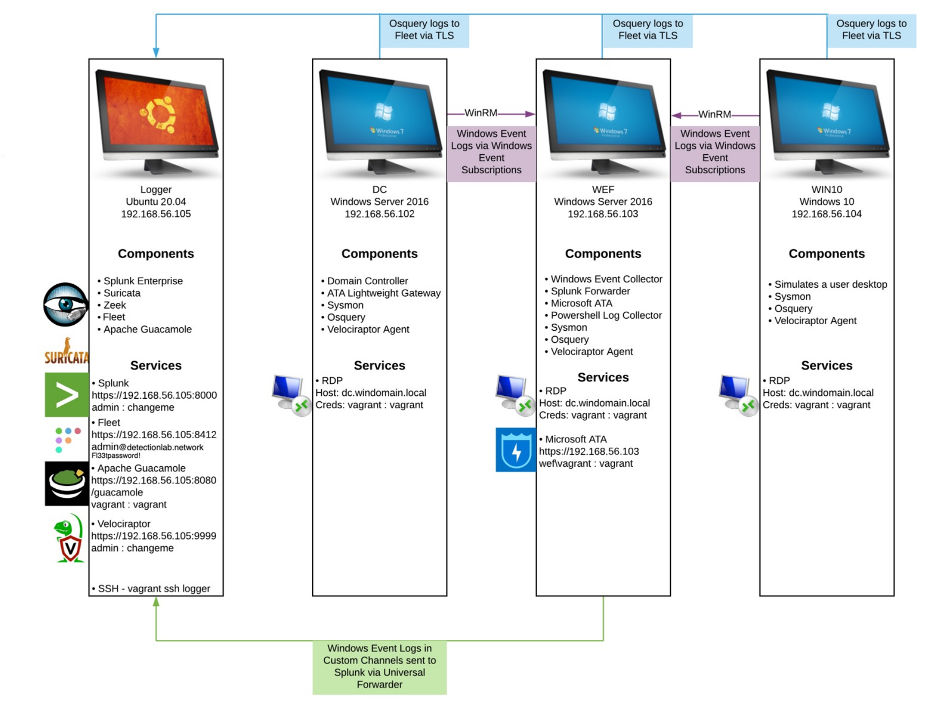
17



NOW WHAT PART 2

- VulnHub - https://www.vulnhub.com/
- Metasploitable 2 & 3
- Detection Lab! - https://www.detectionlab.network
  - Proxmox Deployment!xs
- 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

18



Osquery logs to Fleet via TLS

Osquery logs to Fleet via TLS

Osquery logs to Fleet via TLS

WinRM

Windows Event Logs via Windows Event Subscriptions

WinRM

Windows Event Logs via Windows Event Subscriptions

Logger
Ubuntu 20.04
192.168.56.105

Components

- Splunk Enterprise
- Suricata
- Zeek
- Fleet
- Apache Guacamole

Services

- Splunk
  https://192.168.56.105:8000
  admin : changeme
- Fleet
  https://192.168.56.105:8412
  admin@detectionlab.network
  Fl33tpassword!
- Apache Guacamole
  https://192.168.56.105:8080
  /guacamole
  vagrant : vagrant
- Velociraptor
  https://192.168.56.105:9999
  admin : changeme
- SSH - vagrant ssh logger

DC
Windows Server 2016
192.168.56.102

Components

- Domain Controller
- ATA Lightweight Gateway
- Sysmon
- Osquery
- Velociraptor Agent

Services

- RDP
  Host: dc.windomain.local
  Creds: vagrant : vagrant

WEF
Windows Server 2016
192.168.56.103

Components

- Windows Event Collector
- Splunk Forwarder
- Microsoft ATA
- Powershell Log Collector
- Sysmon
- Osquery
- Velociraptor Agent

Services

- RDP
  Host: dc.windomain.local
  Creds: vagrant : vagrant
- Microsoft ATA
  https://192.168.56.103
  wef\vagrant : vagrant

WIN10
Windows 10
192.168.56.104

Components

- Simulates a user desktop
- Sysmon
- Osquery
- Velociraptor Agent

Services

- RDP
  Host: dc.windomain.local
  Creds: vagrant : vagrant

Windows Event Logs in Custom Channels sent to Splunk via Universal Forwarder

19

NOW WHAT PART 3

- Parrot OS vs Kali
- Tenable
- OpenVAS
  - Note - /etc/postgresql/13/main/postgresql.conf, 5432, restart
  - (kali-tools-vulnerability)
  - gvm-setup
- K8s/k3s
  - k3sup - https://github.com/alexellis/k3sup
  - Rancher - https://rancher.com/docs/rancher/v2.x/en/installation/install-rancher-on-k8s/
- HomePwn - https://github.com/Telefonica/HomePWN
- https://pwnagotchi.ai/ - Pi Zero!

20

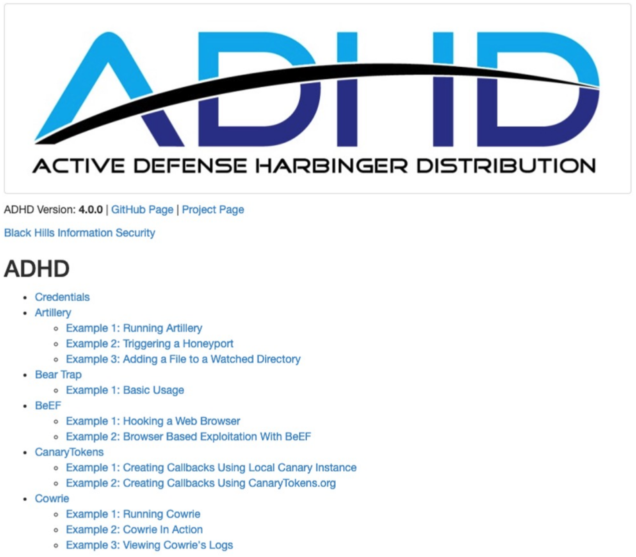
HONEYPOTS!

- 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..

21

ADHD



ACTIVE DEFENSE HARBINGER DISTRIBUTION

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

Black Hills Information Security

ADHD

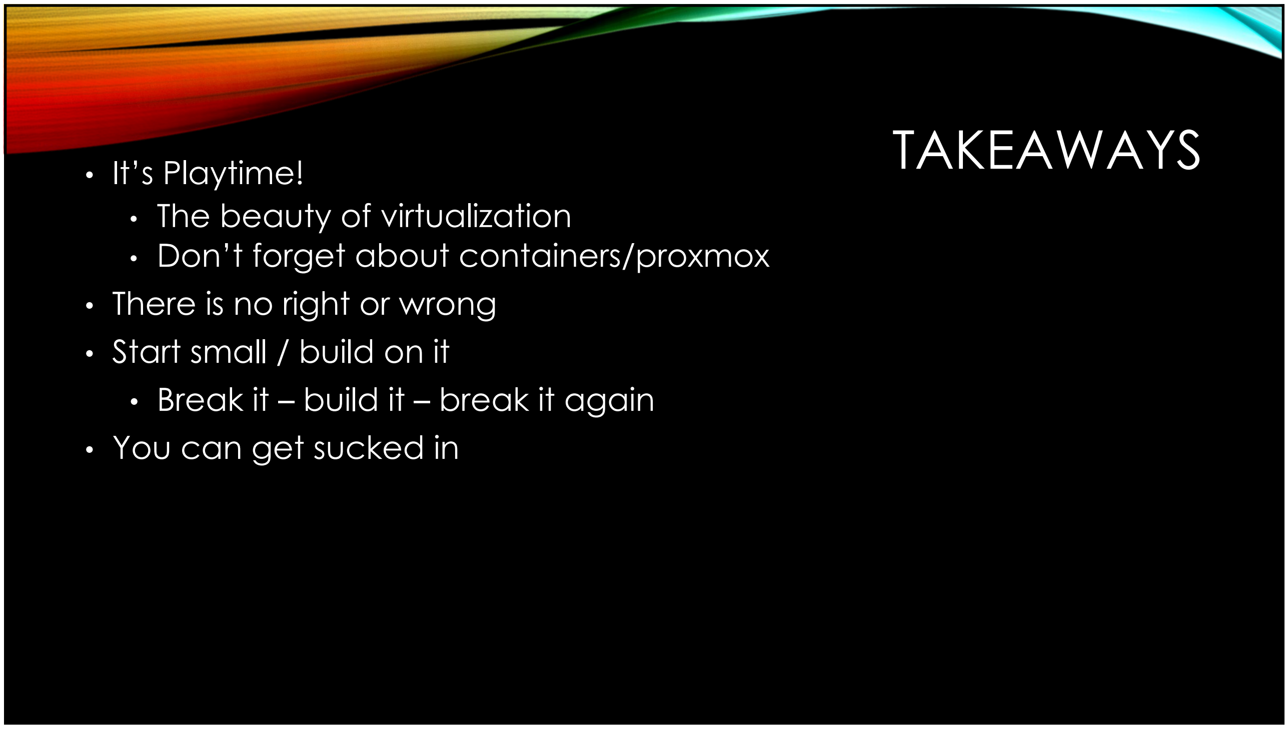
- Credentials
- Artillery
  - Example 1: Running Artillery
  - Example 2: Triggering a Honeyport
  - Example 3: Adding a File to a Watched Directory
- Bear Trap
  - Example 1: Basic Usage
- BeEF
  - Example 1: Hooking a Web Browser
  - Example 2: Browser Based Exploitation With BeEF
- CanaryTokens
  - 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

22

FINDING PEERS

- DefCon
  - Diana Initiative
- BSides
- CFPs
- CTFs
- tryhackme.com
- hackthebox.com

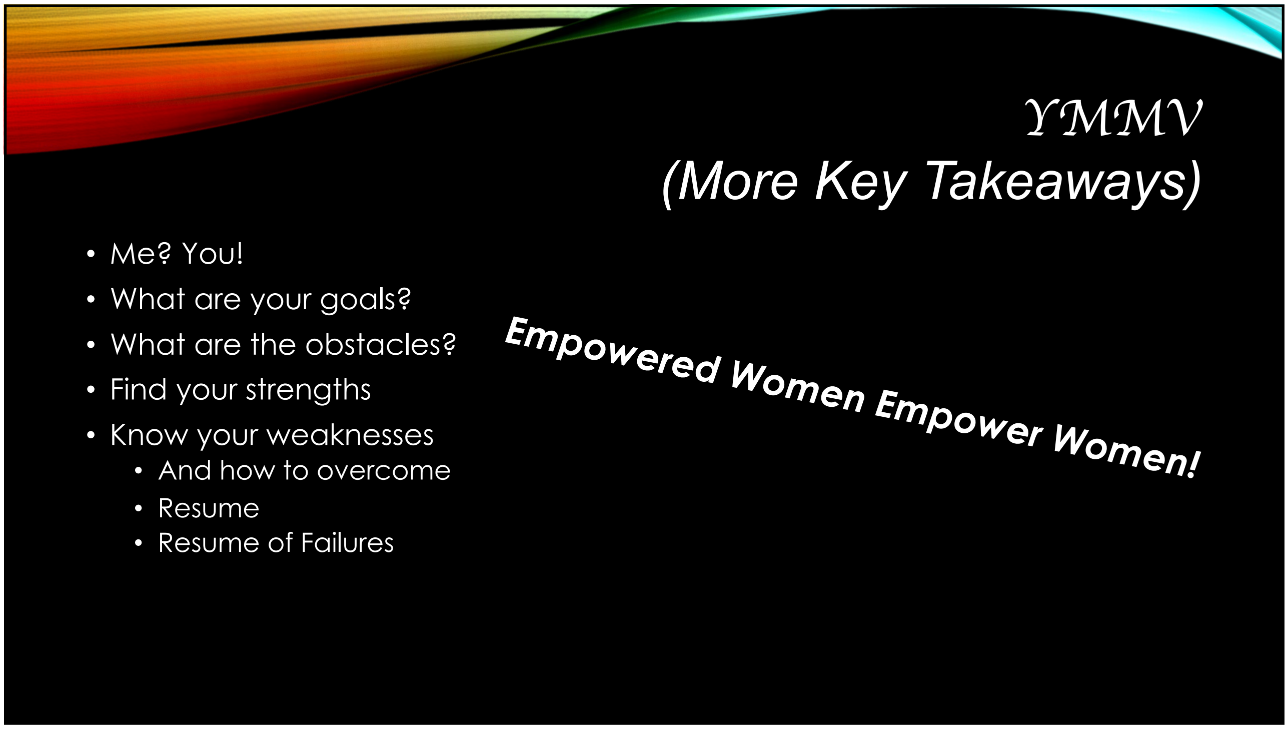
23



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

24



YMMV
(More Key Takeaways)

- Me? You!
- What are your goals?
- What are the obstacles?
- Find your strengths
- Know your weaknesses
  - And how to overcome
  - Resume
  - Resume of Failures

Empowered Women Empower Women!

25

THANK YOU

Kat Fitzgerald
evilkat@rnbwmail.com

@rnbwkat
@rnbwkat@infosec.exchange

LinkedIN - katfitzgerald

WHY
WHERE
HOW
WHEN
WHERE
WHY
WHO
WHAT
WHAT
WHEN
WHAT
WHEN
WHERE
HOW
WHY
?

26