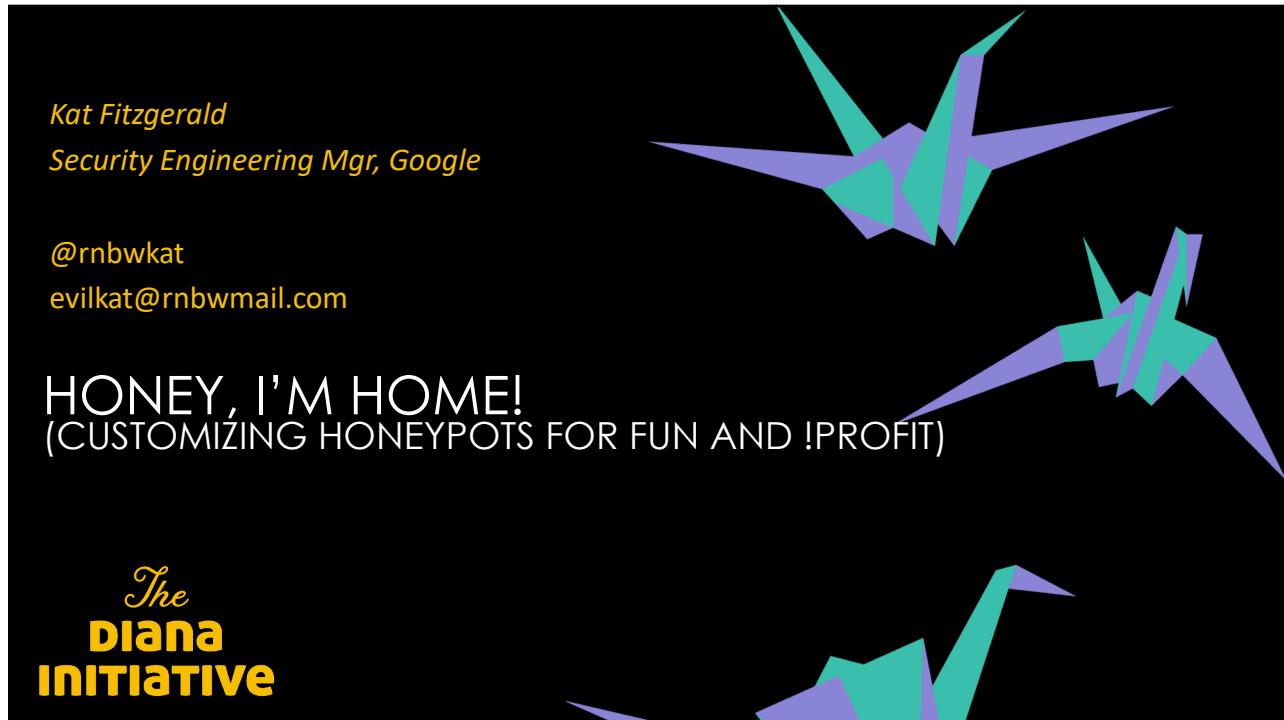




2



3

\$ whoami

- CEO @BSidesChicago,
2019 COO @dianainitiative,
CFP Chair @BSidesPGH, DefCon 3!
- Based in Kirkland, WA 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

4

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 within this presentation are only examples and they should not be utilized in the real-world.

5

WHY WE ARE NOT HERE

- This is not a demo of 5000 different honeypots
- I'm not showing you all my honeypots (duh)
- Honeypots are only PART of your Security Posture



6

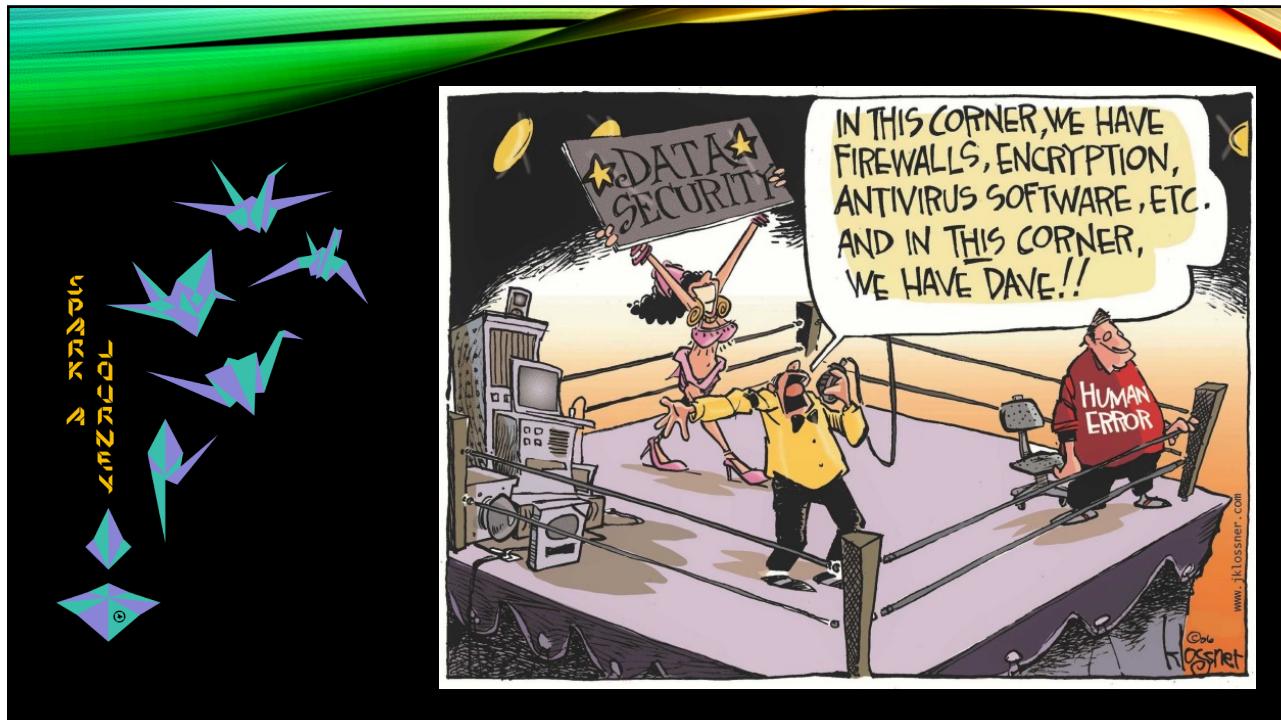
WHY WE ARE HERE

- Spending exceeded \$123 billion - 2020
- Attacks and breaches are commonplace
- Security “stuff” is vulnerable
- Lateral Movement – (*this will become more important*)
- But what about –
 - Your Security Architecture is not unique
 - What is your “typical day”

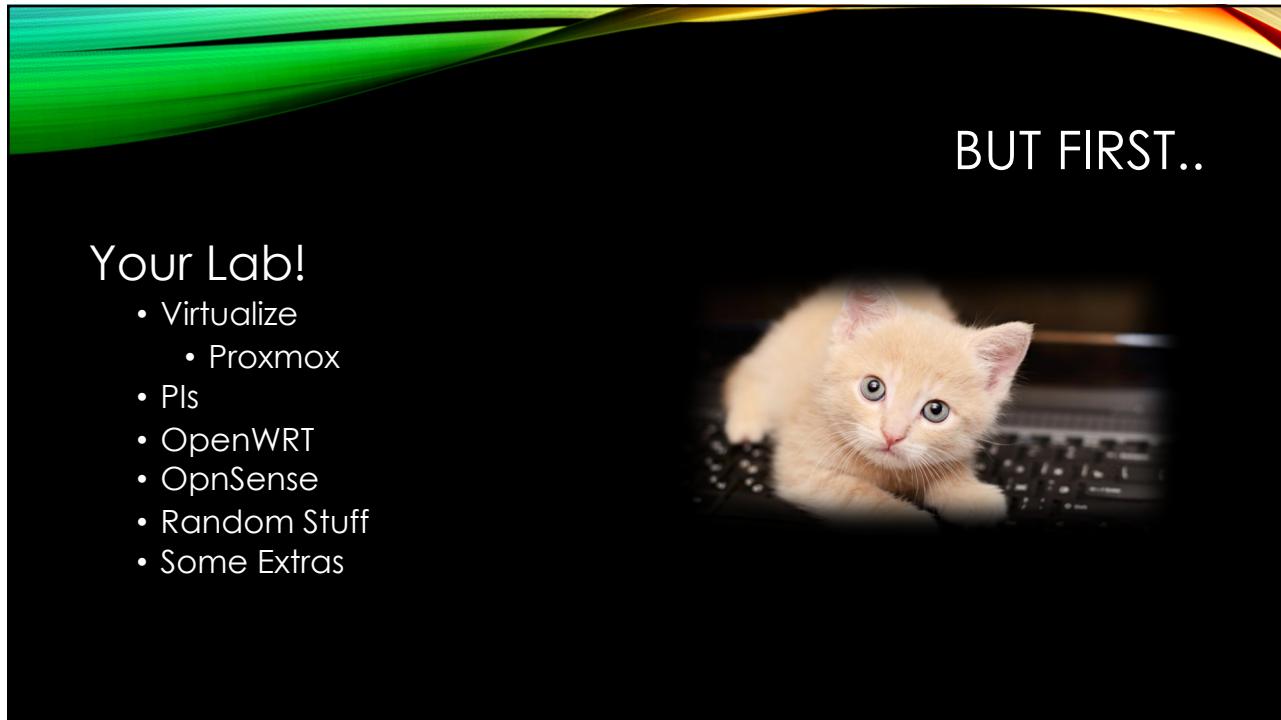


Instead of Brilliance, we have standardized mediocrity.
– John Strand, Offensive Countermeasures

7



8



9

HONEYPOTS



- Honeypots vs Deception
 - A resource with no value(?)
 - Value = Use of Resource
 - Does Not Hack Back

- Important Points
 - Deployment
 - Customization = Planning! (more on this)
 - 100's of "types"

10

PICK ONE

- OpenCanary -- <https://opencanary.readthedocs.io/en/latest/>
- Adhd – <https://www.activecountermeasures.com/free-tools/adhd/>
- Honey Badger -- <https://github.com/adhdproject/honeybadger> (GEO!)
- CHN-- <https://communityhoneynetwork.readthedocs.io/en/stable/>
- Canarytokens -- <https://canarytokens.org/generate>
- T-pot -- <https://github.com/telekom-security/tpotce>
- Cowrie -- <https://github.com/cowrie/cowrie>
- PIs w/lights -- <https://github.com/mattymcfatty/HoneyPi>
- Lots more -- <https://github.com/paralax/awesome-honeypots>

- What about the “Real Thing”? Hmm..

11



ADHD Version: 4.0.0 | [GitHub Page](#) | [Project Page](#)
Black Hills Information Security

ADHD

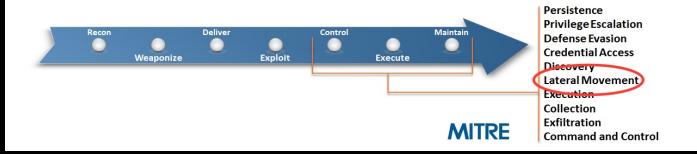
- Credentials
- Artillery
 - Example 1: Running Artillery
 - Example 2: Triggering a Honeyport
 - Example 3: Adding a File to a Watched Directory
- Bear Trap
 - Example 1: Basic Usage
- BeEF
 - Example 1: Hooking a Web Browser
 - Example 2: Browser Based Exploitation With BeEF
- CanaryTokens
 - Example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

<https://www.activecountermeasures.com/free-tools/adhd/>

12

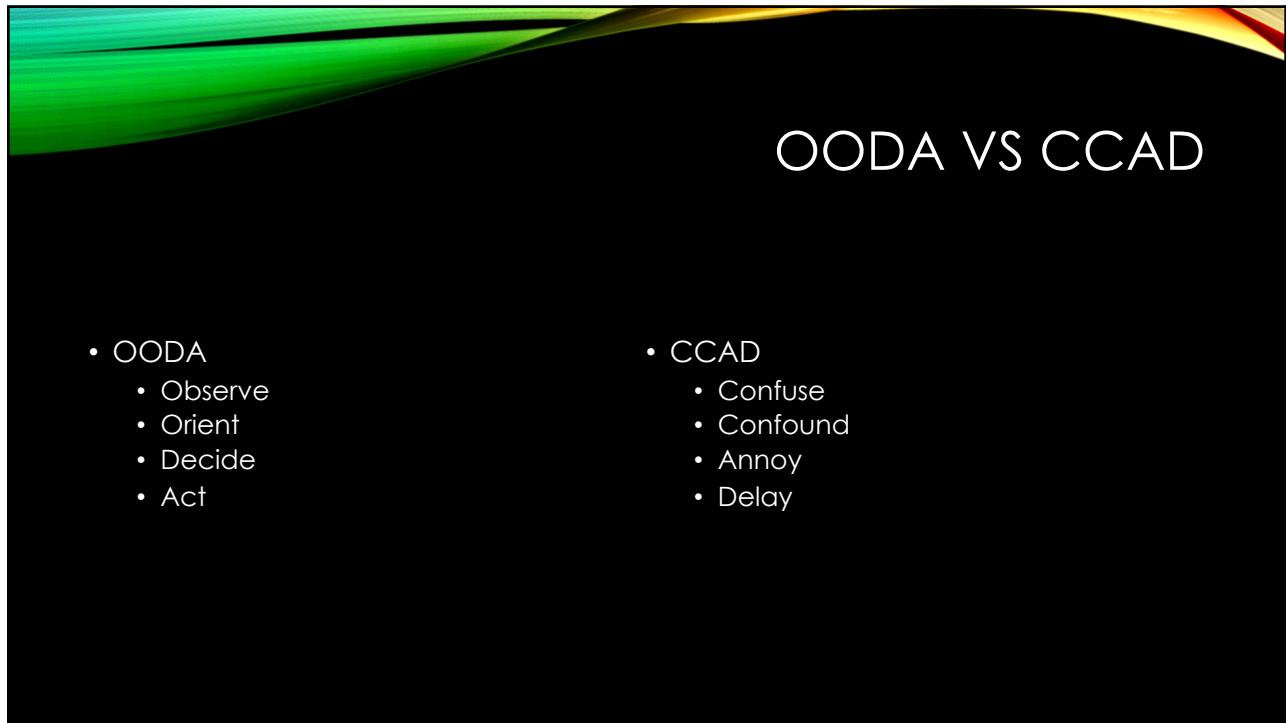
LATERAL MOVEMENT

- Enables an adversary to access and control remote systems on a network.
- *(See, I told you it would become important later)*



The diagram illustrates the MITRE ATT&CK framework. It shows a horizontal timeline with phases: Recon, Weaponize, Deliver, Exploit, Control, Execute, and Maintain. A large blue arrow points from left to right, indicating the flow of the attack. The 'Control' and 'Execute' phases are grouped together. To the right of the timeline is a vertical list of tactics. An orange line connects the 'Control' phase to the 'Lateral Movement' tactic, which is circled in red. The tactics listed are: Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Execution, Collection, Exfiltration, and Command and Control. The MITRE logo is at the bottom of the list.

13



14

MONITORING
wazuh.com

Log data analysis

Attack tactics by agent

agent.name	Credential Access	Defense Evasion	Execution	Lateral Movement	Persistence
Ubuntu	~30,000	~25,000	~20,000	~15,000	~10,000
CentOS	~25,000	~20,000	~18,000	~12,000	~8,000
Debian	~30,000	~28,000	~22,000	~18,000	~12,000
macOS	~20,000	~18,000	~15,000	~10,000	~8,000
Windows	~30,000	~25,000	~20,000	~15,000	~10,000

Exploit Public-Facing Application

ID	Tactic	Platform	Data sources
T1190	Initial Access	AWS, Azure, GCP, Linux, Windows, macOS	Azure activity logs, AWS CloudTrail logs, Stackdriver logs, Packet capture, Web logs, Web application firewall logs, Application logs

Recent events

Time	Technique(s)	Tactic(s)	Level	Rule ID	Description
2020-08-19 07:45:04	T1190	Initial Access	5	30306	Apache: Attempt to access forbidden directory index.

Information

ID	Level	File	File
30106	5	0250-apache_rules.xml	ruleset_name

Details

if_sid	Match
30101	Directory index forbidden by rule

Compliance

PCI DSS	GDPR	HIPAA	NIST-800
6.5.2, 10.2.4	Iv_35.7.d	164.312.b	SA.11, AU.1

Related rules

ID	Description	Groups	Compliance	Level
30104	Apache segmentation fault.	service_availability, apache, web	PCI, HIPAA, GDPR, NIST-800-53 TSC	12

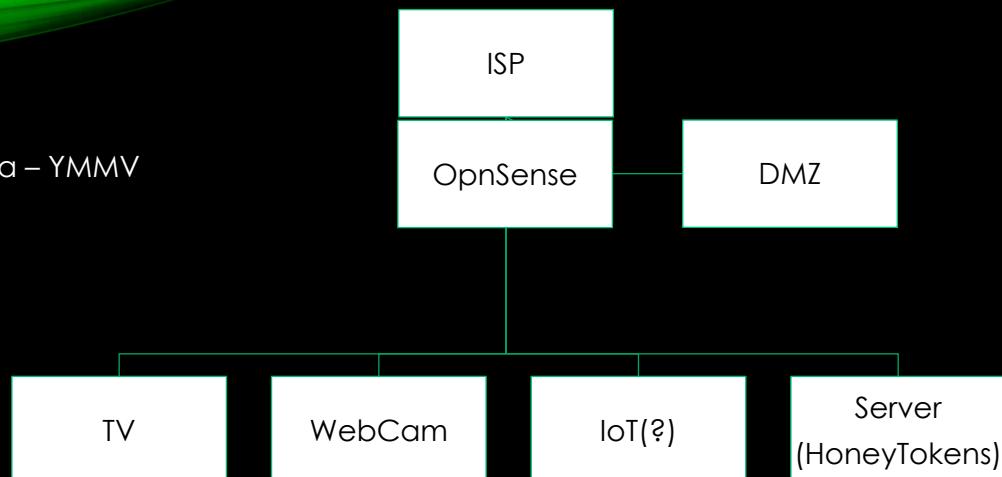
15

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

16

- An Idea – YMMV



```
while true ; do nc -l -p 1500 -c 'echo -e "HTTP/1.1 200 OK\n\n $(date)"'; done
```

17

LET'S TALK CUSTOMIZATION

- Think
 - Over = No!
- What?
- Look around
- eBay = fun times
 - Wifi – old
 - Cameras
 - Enable ssh
- Shodan
- Where – more on this later

18

CUSTOMIZATION

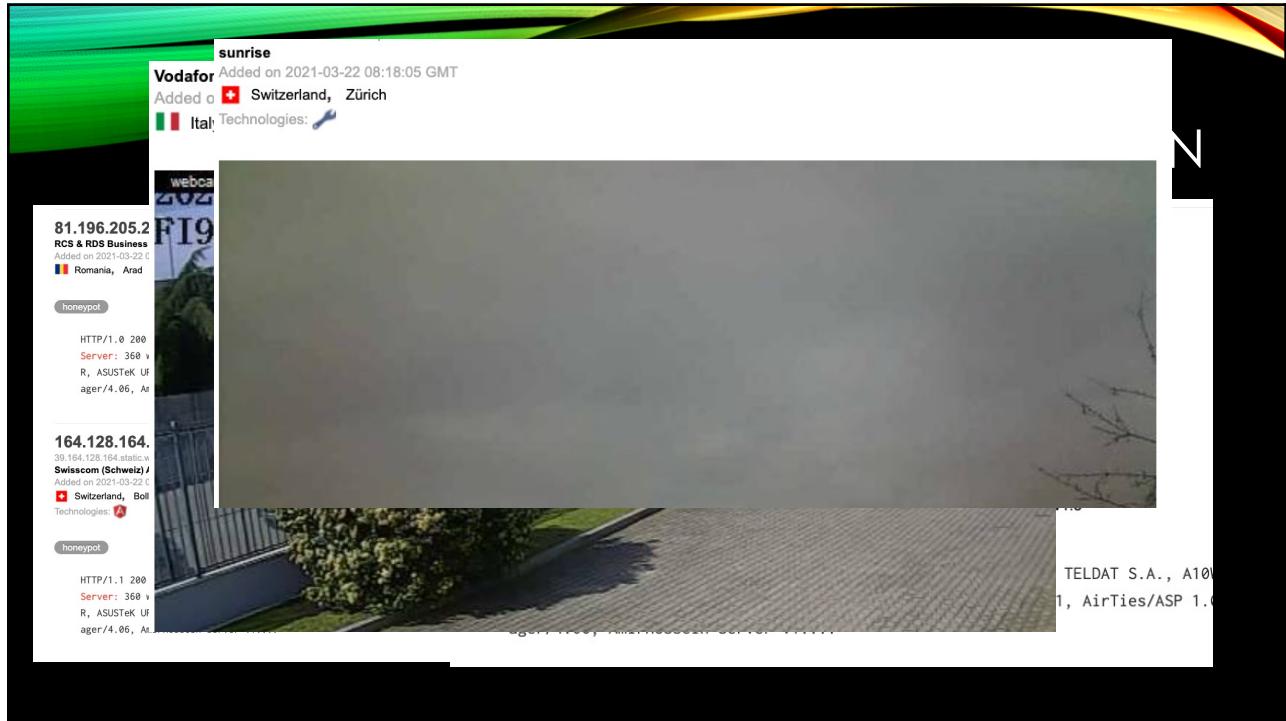
- Start with your (friends? Neighbors?) devices
- Shodan
 - Banners
 - Versions!
 - HTML
- Certificates
- HoneyTokens
- Hosts
 - Filesystems
 - Commands
 - History
 - Processes
 - HoneyTokens
- Real Servers and Apps
 - Staging

Too legit to quit!!

Make it look real!

*Rename built-in user richard to phil,
it's used as detection mechanism.*

19



20

FOR REAL?

- Why not use real software?
- RDP
 - Honeytokens
 - Honeydocs
- Think about “discovery”?
- Don’t forget monitoring agent (Wazuh)

21

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

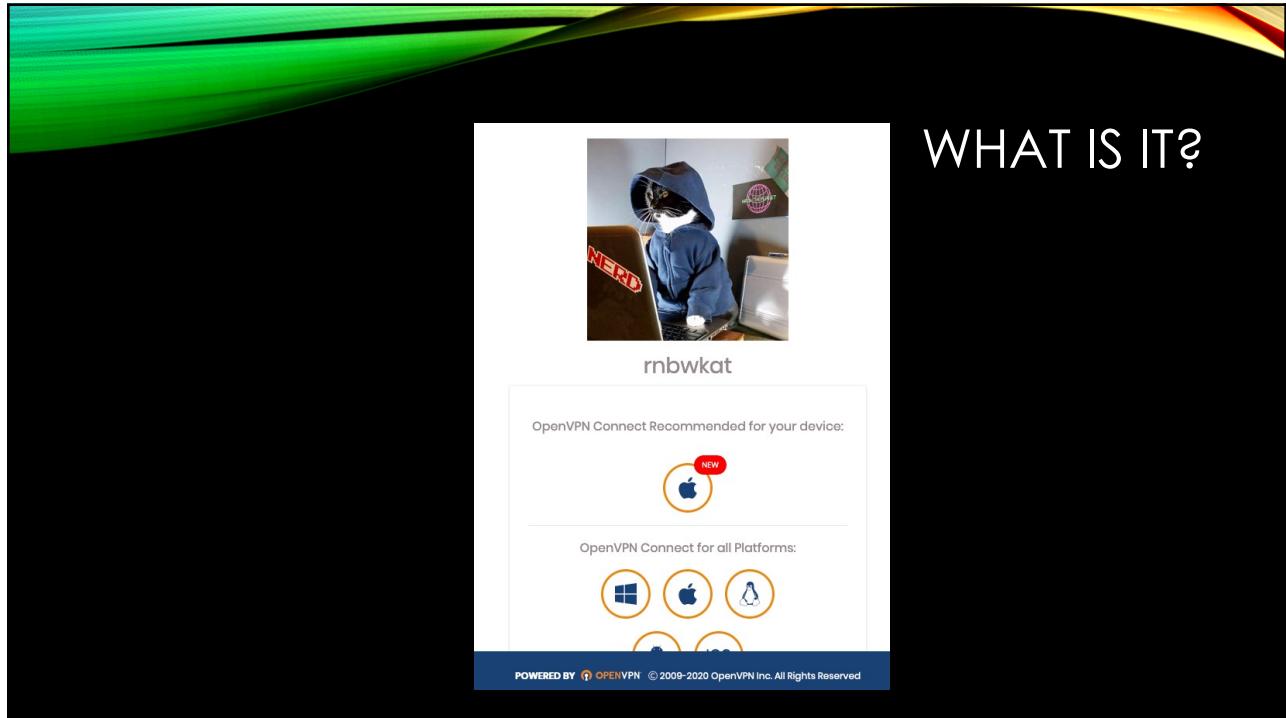
# df
Filesystem      1K-blocks      Used Available Use% Mounted on
rootfs          40960       40960        0 100% /
/dev/root       40960       40960        0 100% /
devtmpfs        257456         0   257456   0% /dev
tmpfs           257600       944   256656   0% /tmp
/dev/mtdblock4    65536      2064     63472   3% /jffs
```

22

COWRIE

```
# ls -al /etc
srwxrwxrwx  1 admin  root          0 May  5 2018 amas_lib_socket
-rw-rw-rw-  1 admin  root      1017 May  5 2018 cert.pem
drwxrwxrwx  2 admin  root        100 May  5 2018 cfg_mnt
srwxrwxrwx  1 admin  root          0 May  5 2018 cfgmnt_ipc_socket
-rw-rw-rw-  1 admin  root      380 May  5 2018 dnsmasq.conf
drwx-----  2 admin  root      100 Feb 27 13:24 dropbear
lrwxrwxrwx  1 admin  root      20 Dec 31 1969 e2fsck.conf -> /rom/etc/e2fsck.conf
drwxrwxrwx  2 admin  root       60 May  5 2018 email
lrwxrwxrwx  1 admin  root      19 Dec 31 1969 ethertypes -> /rom/etc/ethertypes
-rw-r--r--  1 admin  root          0 Dec 31 1969 fstab
-rw-r--r--  1 admin  root      52 May  5 2018 group
-rw-rw-rw-  1 admin  root          0 May  5 2018 group.custom
-rw-r--r--  1 admin  root      52 May  5 2018 gshadow
-rw-r--r--  1 admin  root      176 May  5 2018 hosts
lrwxrwxrwx  1 admin  root      23 Dec 31 1969 hotplug2.rules -> /rom/etc/hotplug2.rules
-rw-r--r--  1 admin  root      365 May  5 2018 ipsec.conf
drwxr-xr-x 10 admin  root      200 May  5 2018 ipsec.d
-rw-rw-rw-  1 admin  root     1675 May  5 2018 key.pem
```

23



24

MORE CUSTOMIZATION

Cowrie

- The obvious
 - Hostname (and MAC!)
 - openssl rand -hex 6 | sed 's/\(..\)/\1:/g; s/:\$//'
 - Versions
 - History
 - Commands
 - History -s (or just copy .bash_history)
 - Targets?
 - Filesystem
 - Processes
 - Usernames
 - Honeycreds

*Remember Proxmox?
Monitoring!*

25

CUSTOMIZATION EXAMPLES

- Banners = easy, but don't forget ssh headers/ciphers/version
- Ping?
- DNS?
- rsync is your friend – honeyfs / createsfs
- ps a running system (cmdoutput.json)
 - Command, cpu, mem, pid, rss, start, stat, time, tty, user, vsz

```
$ ps -eo pcpu,%mem,pid,rss,start_time,stat,bsdttime,tty,user,vsz,args
%CPU %MEM PID RSS START STAT TIME TT USER VSZ COMMAND
0.0 0.0 14995 4456 03:32 S 0:00 ? dovecot 50052 dovecot/imap-login [67.18.92.27 TLS proxy]
0.0 0.0 15034 3500 03:32 S 0:00 ? dovecot 49784 dovecot/imap-login
0.2 0.0 15154 91232 03:35 S1 0:51 ? apache 383516 /usr/sbin/httpd -DFOREGROUND
0.0 0.0 15233 0 Feb04 S< 0:00 ? root 0 [kworker/22:1H]
0.0 0.0 15525 4868 Feb04 Ss 6:14 ? root 279644 php-fpm: master process
(/usr/local/emp3s/etc/php-fpm.conf)
0.0 0.0 15533 6816 Feb04 S 0:00 ? emp3s 280408 php-fpm: pool ordinary
0.0 0.0 15538 408 Feb04 Ss 0:00 ? root 20828 nginx: master process
/usr/local/emp3s/sbin/nginx -c /usr/local/emp3s/etc/nginx/nginx.conf
```

26

CUSTOMIZATION EXAMPLES (CONT)

- Users/passwords
 - rockyou
 - rockyou2021
 - Of course, default
 - Get creative with users
 - htpasswd
- Other “places”
 - Remember the real services/apps?
 - smb
 - rdp
 - ftp/ftps
- pwned

It would take a computer about
7 QUADRILLION YEARS
 to crack your password

27



REMEMBER

84%

of organizations breached had evidence of the breach in their log files...

Source: Verizon Data Breach Report, 2014

28



TAKEAWAYS

- CCAD
- Low False Positives
 - Defend & Detect
- Lateral Movement
- Cost Effective
- Forensics
- REAL Threat Intelligence
 - It's About Thinking Differently, not "watching everything"

29

THANK YOU!!!

- Kat Fitzgerald

- @rnbwkat

- evilkat@rnbwmail.com

