CUSTOMIZING HONEYPOTS

Kat Fitzgerald
Security Engineering Mgr

@rnbwkat
evilkat@rnbwmail.com

1

$ 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*

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

3

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

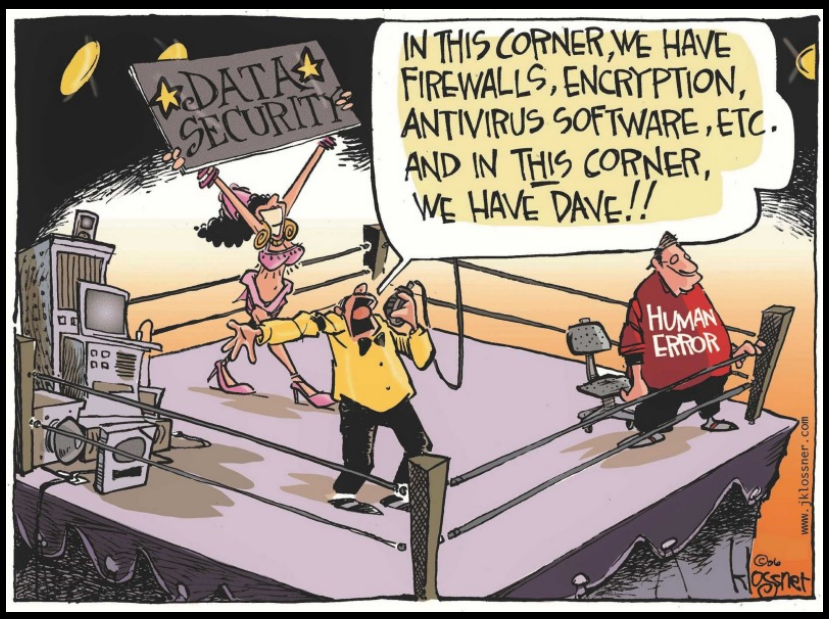
4

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"

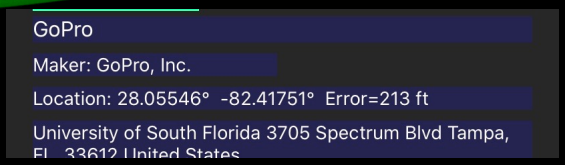
Instead of Brilliance, we have standardized mediocrity.
– John Strand, Offensive Countermeasures

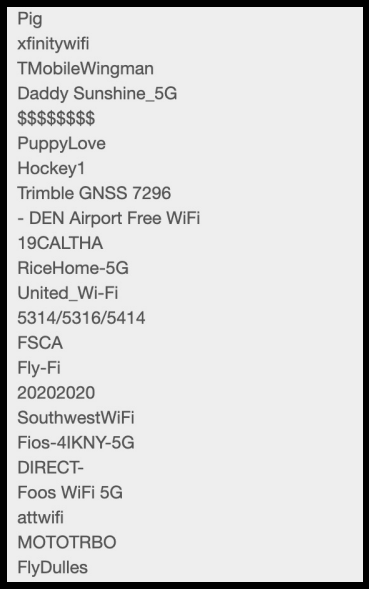
5



6

And…





7

EXAMPLES

- University attacked by its lightbulbs, vending machines and lamp posts
- Industrial
  - Shut down an Oil Rig
  - Blast Furnace
  - Toilet

8

BUT FIRST..

Your Lab!

- Virtualize
  - Proxmox
- PIs
- OpenWRT
- OpnSense
- Random Stuff
- Some Extras

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"? Hmmmm..

11

ADHD

ACTIVE DEFENSE HARBINGER DISTRIBUTION

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

Black Hills Information Security

ADHD

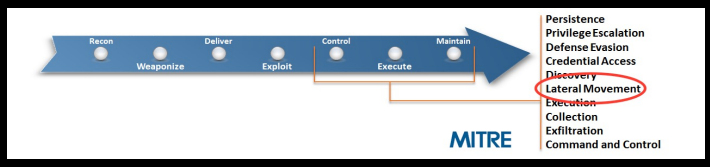
- Credentials
- Artillery
  - Example 1: Running Artillery
  - Example 2: Triggering a Honeyport
  - Example 3: Adding a File to a Watched Directory
- Bear Trap
  - Example 1: Basic Usage
- BeEF
  - Example 1: Hooking a Web Browser
  - Example 2: Browser Based Exploitation With BeEF
- CanaryTokens
 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

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)*



13

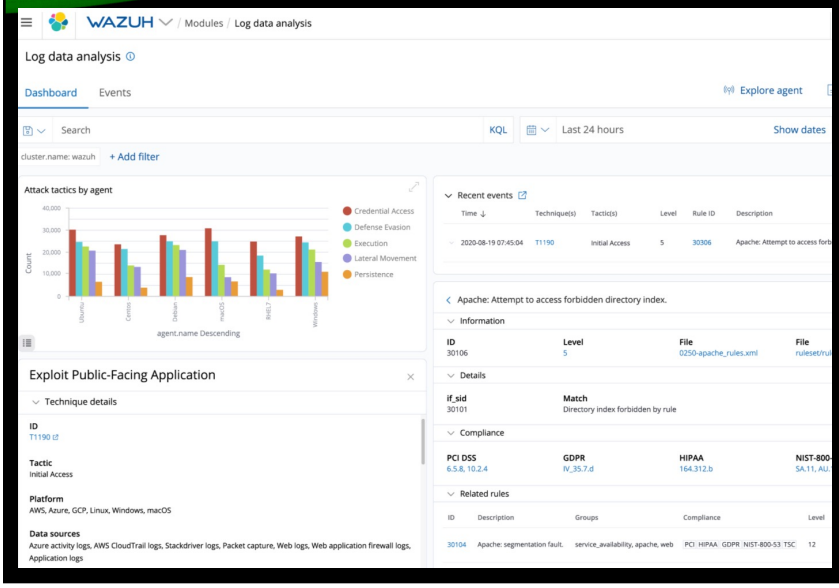
OODA VS CCAD

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

14

MONITORING

wazuh.com



15

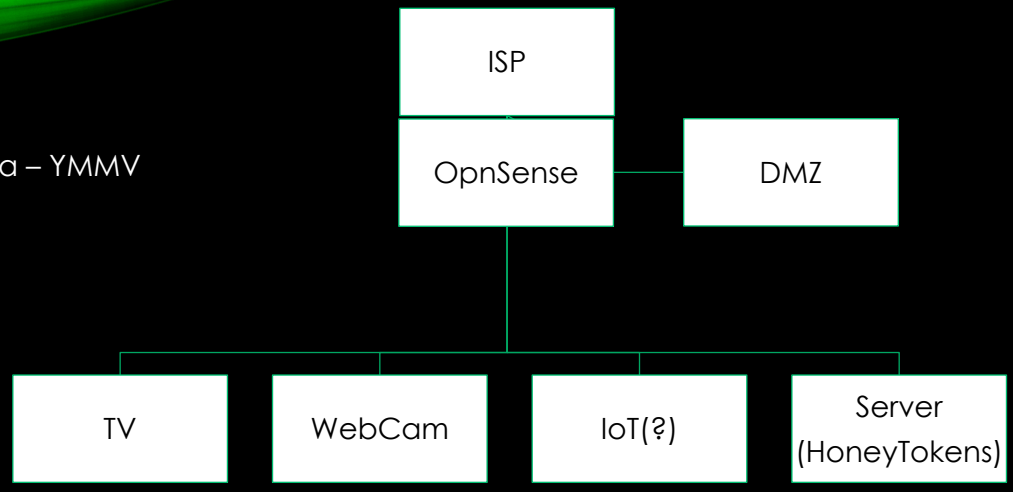
DEPLOYMENT

- 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

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.

18


sunrise
Added on 2021-03-22 08:18:05 GMT
Switzerland, Zürich
Technologies:
81.196.205.2
RCS & RDS Business
Romania, Arad
honeypot
HTTP/1.0 200
164.128.164.
Swisscom (Schweiz)
Switzerland,
honeypot
HTTP/1.1 200
TELDAT S.A.,
AirTies/ASP

19


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

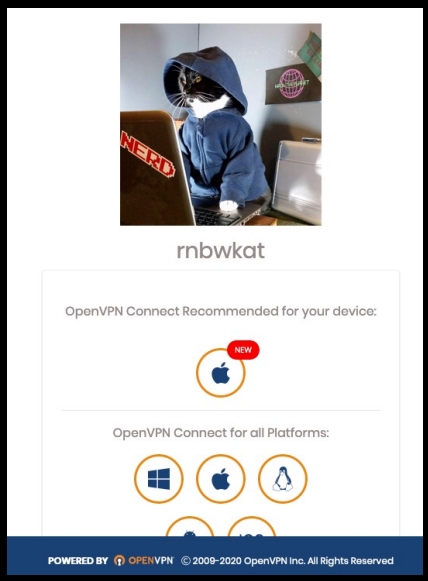
20

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
```

21

WHAT IS IT?



22

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)
  - Filesystem
  - Processes
  - Usernames
    - Honeycreds

Monitoring!

23

CUSTOMIZATION EXAMPLES

- Banners = easy, but don't forget ssh headers/ciphers/version
- Ping?
- rsync is your friend – honeyfs / createfs
- 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,bsdtime,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 Sl     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/emps/etc/php-
fpm.conf)
 0.0  0.0 15533  6816 Feb04 S      0:00 ?        emps     280408 php-fpm: pool ordinary
 0.0  0.0 15538   408 Feb04 Ss     0:00 ?        root      20828 nginx: master process /usr/local/emps/sbin/nginx -c
/usr/local/emps/etc/nginx/nginx.conf
```

24

HIDING IN PLAIN SIGHT

84%

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

Source: Verizon Data Breach Report, 2014

25

TAKEAWAYS

- CCAD
- Low False Positives
  - Defend & Detect
- Lateral Movement
- Cost Effective
- Forensics
- REAL Threat Intelligence
  - It's About Thinking Differently, not "watching everything"
- https://github.com/ElevenPaths/HomePWN
  HomePwn - Swiss Army Knife for Pentesting of IoT Devices

26

27