



1



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

DISCLAIMER (PART 2)

- I'm obsessed(?) with home security equipment, honeypots and colos
- If you want to have a life, perhaps tone it down a bit
- YMMV

4

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



5

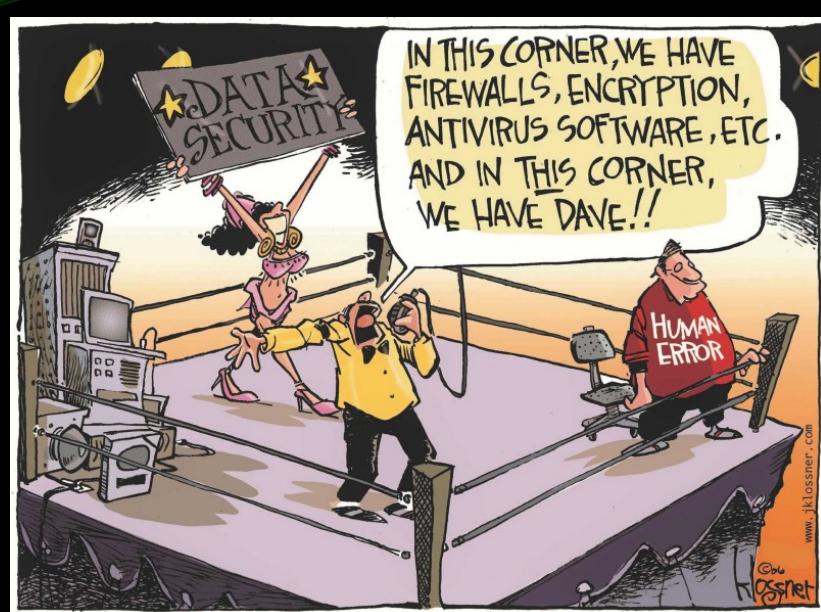
WHY WE ARE HERE

- Spending exceeded \$150 billion - 2021
- 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

6



7

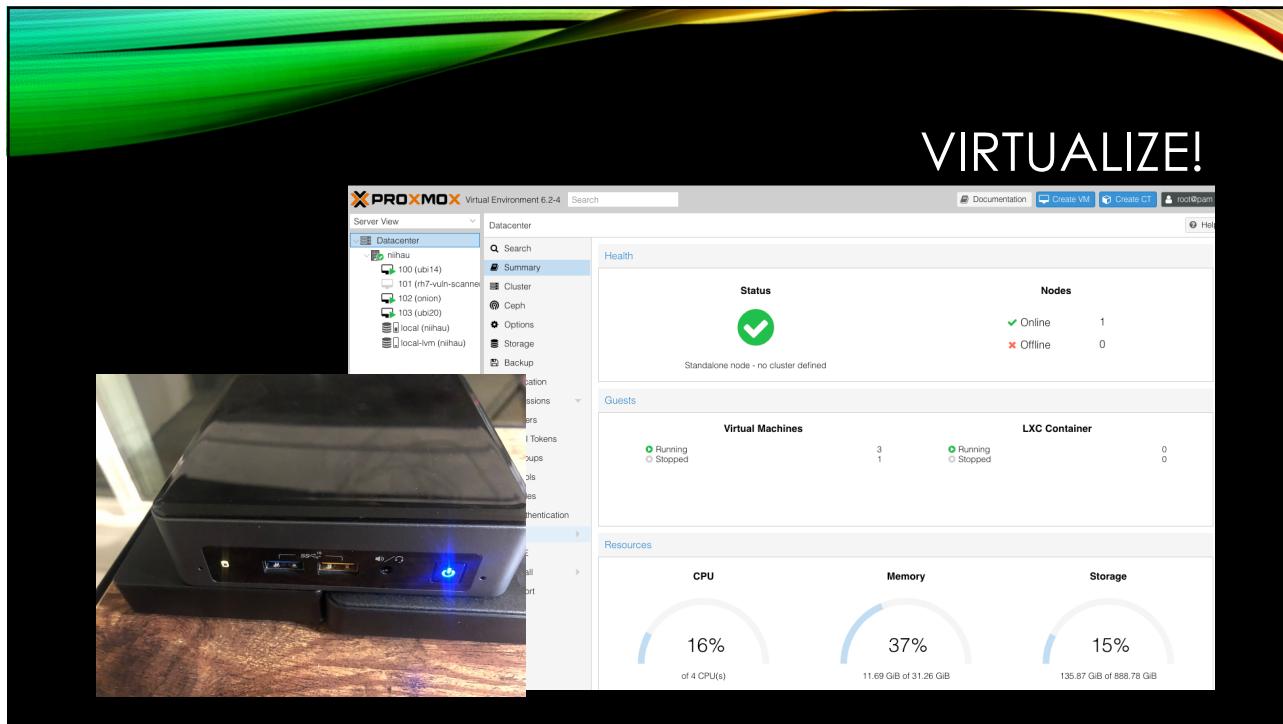
BUT FIRST..

Your Lab!

- Virtualize
 - Proxmox
- Pfs
- OpenWRT (dd-wrt)
- OpnSense
- Random Stuff
- Some Extras



8



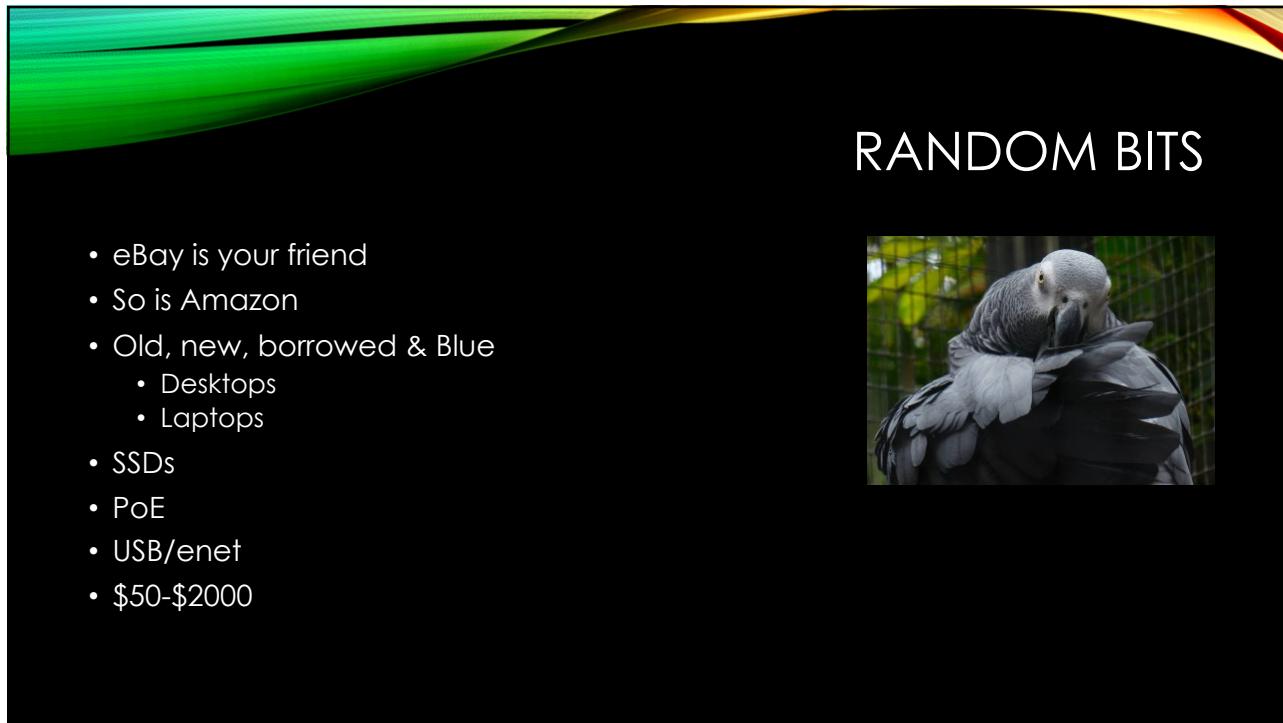
9



10



11



12

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)
- Red Fish / Blue Fish
- Security Onion vs Wazuh



13

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"

14

A FEW.. 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..

15

Remember – do NOT deploy this.
It is for practice and learning only!

Install on a VM such as Virtualbox.



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/>

16

PORTSPOOF (1)

```
nmap -p200-300 gonzo
PORT      STATE SERVICE
200/tcp    open  src
201/tcp    open  at-rtmp
202/tcp    open  at-nbp
203/tcp    open  at-3
204/tcp    open  at-echo
205/tcp    open  at-5
206/tcp    open  at-zis
207/tcp    open  at-7
208/tcp    open  at-8
209/tcp    open  tam
210/tcp    open  z39.50
211/tcp    open  914c-g
212/tcp    open  anet
213/tcp    open  ipx
214/tcp    open  vmpwscs
215/tcp    open  softpc
216/tcp    open  ctls
217/tcp    open  dbase
218/tcp    open  mpp
219/tcp    open  uarps
220/tcp    open  imap3
221/tcp    open  fln-spx
222/tcp    open  rsh-spx
223/tcp    open  cdc
224/tcp    open  masqdialer
```

17

PORTSPOOF (2)

```
nmap -A gonzo
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-27 09:52 EST
Stats: 0:04:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 75.58% done; ETC: 09:58 (0:01:31 remaining)
Stats: 0:04:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 77.22% done; ETC: 09:58 (0:01:26 remaining)
Stats: 0:07:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
```

18

**DSHIELD
5 MINUTES!**

Date	Time	Source	Source Port	Target	Target Port	Protocol
2020-11-19	00:16:59	110.154.181.126	14649	192.168.100.100	23	6
2020-11-19	00:17:26	74.120.14.37	54522	192.168.100.100	23	6
2020-11-19	00:17:31	167.248.133.92	64123	192.168.100.100	23	6
2020-11-19	00:17:31	167.248.133.40	39580	192.168.100.100	23	6
2020-11-19	00:17:31	45.129.33.5	56294	192.168.100.100	23	6
2020-11-19	00:18:03	192.241.217.154	44838	192.168.100.100	23	6
2020-11-19	00:18:31	64.64.104.10	15188	192.168.100.100	23	6
2020-11-19	00:18:43	185.175.93.14	49700	192.168.100.100	23	6
2020-11-19	00:19:14	83.97.20.35	55995	192.168.100.100	23	6

Showing 1 to 100 of 11,920 entries

Previous 1 2 3 4 5 ... 120 Next

19

LATERAL MOVEMENT

- Enables an adversary to access and control remote systems on a network.

The diagram illustrates the MITRE ATT&CK framework. It features a horizontal timeline with arrows pointing from left to right, representing the sequence of operations: Recon, Weaponize, Deliver, Exploit, Control, Execute, and Maintain. A vertical column of techniques is listed on the right, corresponding to each step. The 'Lateral Movement' technique is highlighted with a red oval and a red arrow pointing to it from the 'Control' step in the timeline.

Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Persistence						
Privilege Escalation						
Defense Evasion						
Credential Access						
Discovery						
Lateral Movement						
Execution						
Collection						
Exfiltration						
Command and Control						

MITRE

20

OODA VS CCAD

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

21

MONITORING

wazuh.com
(see appendix)

The screenshot shows the Wazuh Security Events dashboard. On the left, there's a sidebar with navigation links like 'Dashboard', 'Events', 'Logs', 'Metrics', 'Logs', 'Metrics', and 'Logs'. The main area displays a table of security events:

	Description
data.eventid	raju tried to login to honeypot.
data.message	nproc tried to login to honeypot.
data.password	root logged into honeypot.
data.sensor	cowie.login.success
data.session	login attempt [root/password] succeeded
data.src_ip	password
data.timestamp	sasha
data.username	d5c6623bdede
decoder.name	
full_log	redmin tried to login to honeypot.
id	2022-08-07T09:39:50.398166Z
input.type	Integrity checksum changed.
location	root
manager.name	json
rule.description	npoc tried to login to honeypot.
	root logged into honeypot.
	root logged into honeypot.
	jimjarre tried to login to honeypot.
	honeydew
	log
	/home/aladin/cowie/var/log/cowie/cowie

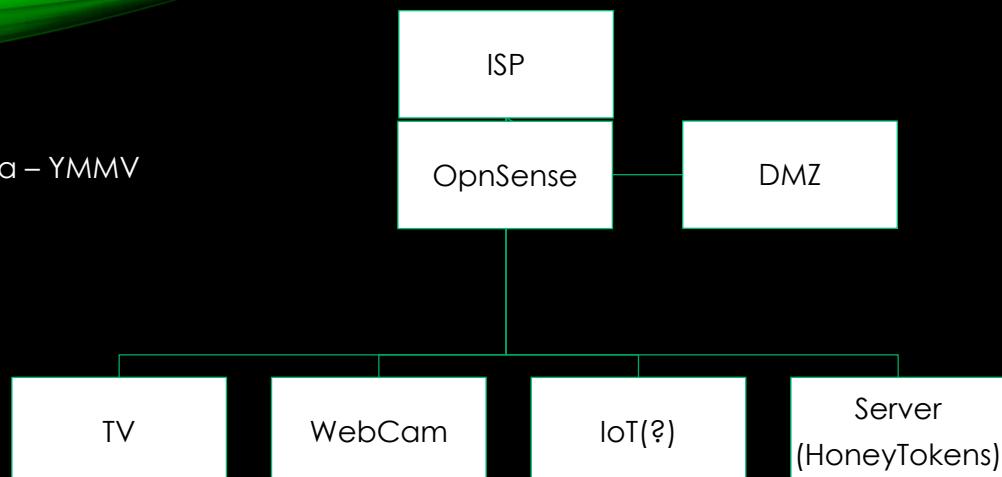
22

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

23

- An Idea – YMMV



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

24

LET'S TALK CUSTOMIZATION

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

25

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.*

26

Server: SQ-WEBCAM

SHODAN

81.196.205.233

RCS & RDS Business
Added on 2021-03-22 02:59:00 GMT
Romania, Arad

honeypot

HTTP/1.0 200 OK
Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., R, ASUSTeK UPnP/1.0 MiniUPnPd/1.4, ATS/5.3.0, Adaptec ASM 1.1, AirTies/ASager/4.06, AmirHossein Server v1....

28ZE

172.105.97.164
li2000-164.members.linode.com
Linode
Added on 2021-03-22 02:46:07 GMT
Canada, Toronto
Technologies:

164.128.164.39

39.164.128.164 static.wilne.ins.ent.cust.swisscom.ch
Swisscom (Schweiz) AG
Added on 2021-03-22 02:13:25 GMT
Switzerland, Bolligen
Technologies:

honeypot

HTTP/1.1 200 OK
Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., A10R, ASUSTeK UPnP/1.0 MiniUPnPd/1.4, ATS/5.3.0, Adaptec ASM 1.1, AirTies/ASP 1.0ager/4.06, AmirHossein Server v1....

SSL Certificate

Issued By:
- Organization: Internet Widgits Pty Ltd

Issued To:
- Organization: Internet Widgits Pty Ltd

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

27

Server: SQ-WEBCAM

SHODAN - 2

honeyscore.shodan.io

jobs Misc Security IoT hPots CTF Pi stuff WiFi Pineapple k8s Cloud Plex ProxMox KVMS TM SAP Cloud

Shodan Scanhub Developers View All...

Honeypot Or Not?
Enter an IP to check whether it is a honeypot or a real control system:

Please enter an IP...

Frequently Asked Questions

- How does it work?
The defining characteristics of known honeypots were extracted and used to create a tool to let you identify honeypots! The probability that an IP has a "Honeyscore" value that can range from 0.0 to 1.0. This is still a prototype/ work-in-progress so if you find some problems please email me at jmath6@protonmail.com
- What's the purpose?

28

FOR REAL?

- Why not use real software?
- RDP
 - Honeytokens
 - Honeydocs
- Think about "discovery"?
- Don't forget monitoring agent!!

29

WHAT IS IT?

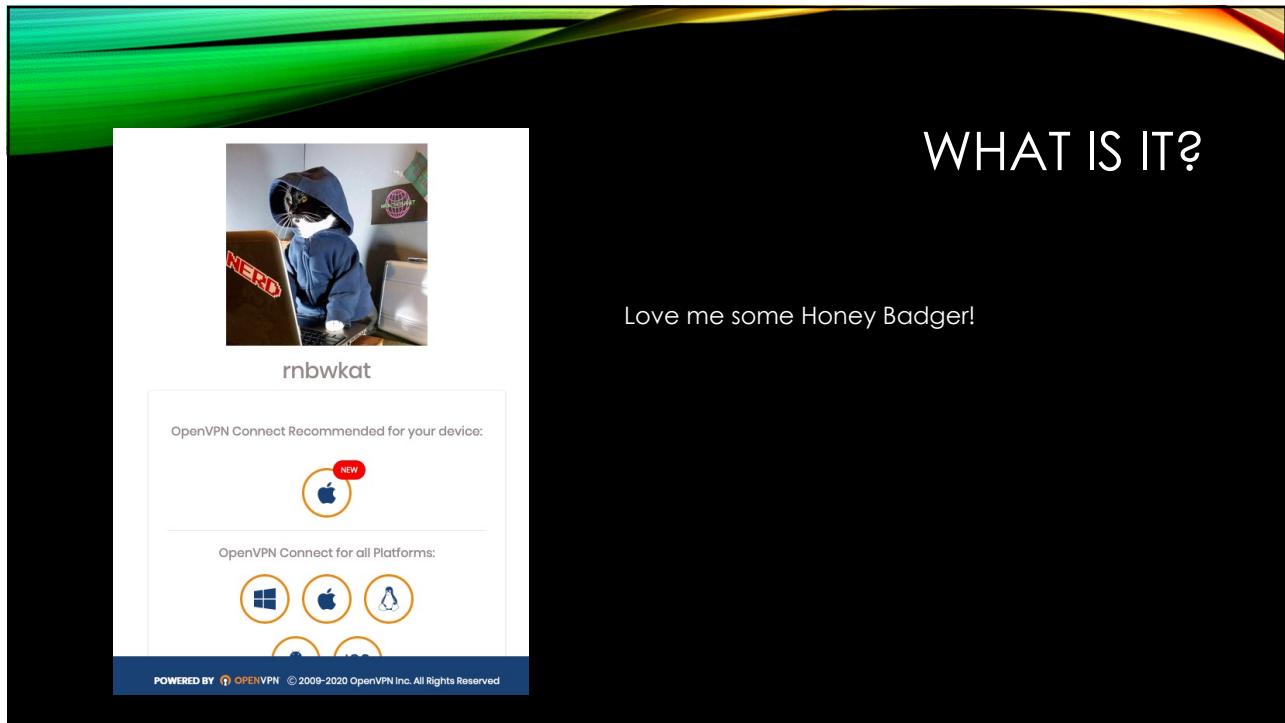
```
# uname -a
Linux RT-AC5300 2.6.36.4brcmarm #1 SMP PREEMPT Fri Oct 18 16:13:51 CST 2019 armv7l
ASUSWRT

# 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
```

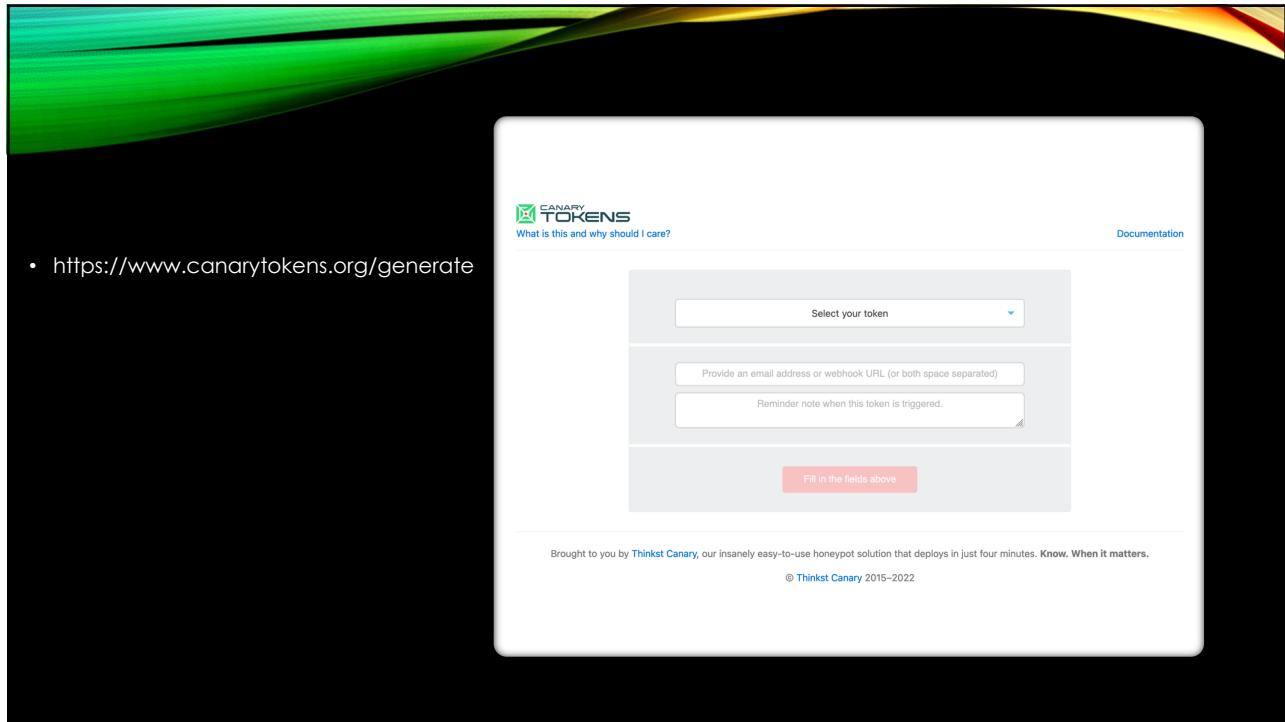
30

```
# 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
```

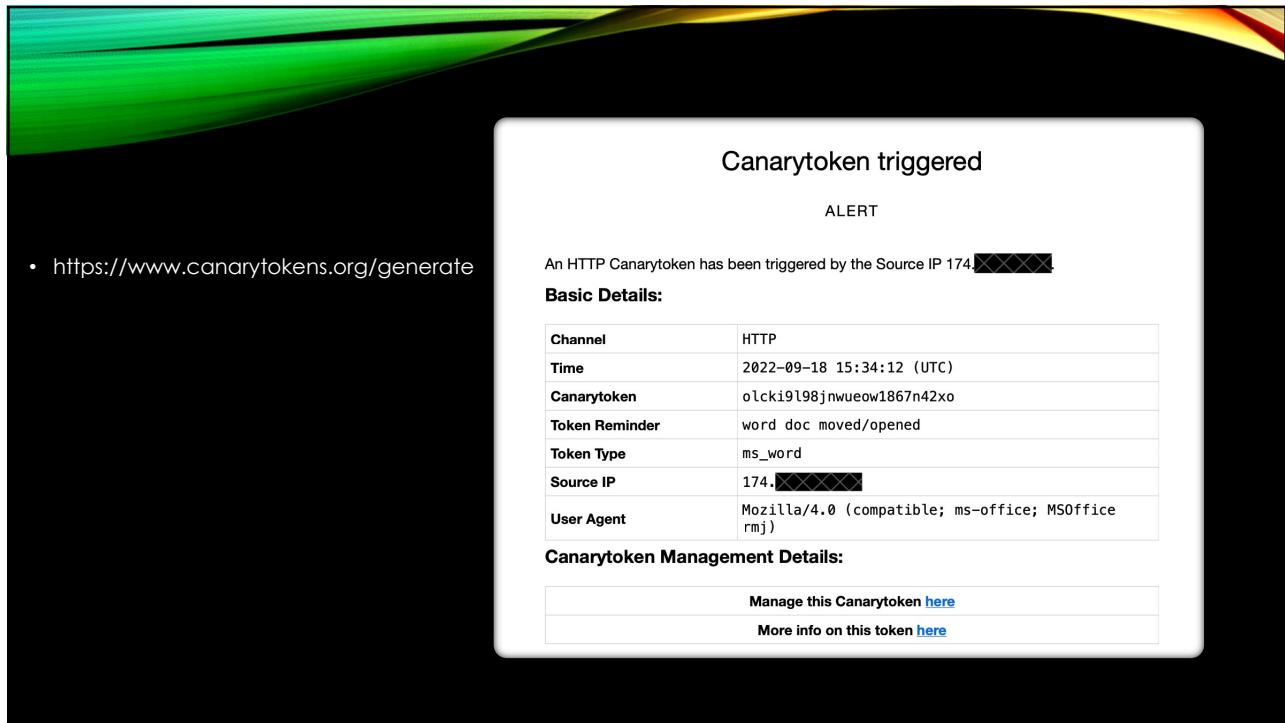
31



32



33



34

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!*

Network

`smsc95xx.macaddr` Tells the smsc95xx driver to use a custom mac address instead of using default mac address.

`smsc95xx.macaddr=B8:AA:BC:DE:F0:12`

35

CUSTOMIZATION EXAMPLES

- Banners = easy, but don't forget ssh headers/ciphers/version
- Ping?
- DNS?
- 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 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/empis/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/empis/sbin/nginx -c /usr/local/empis/etc/nginx/nginx.conf
```

36



LAB

- Build a Cowrie Honeypot to mimic the OS of your choice
 - You need an OS to clone – 192.168.3.112 honey/pots
 - You need an OS to build on – 192.168.3.123:/honeypots (guest)
 - What else?
 - Extra Credit – Canary Token?
 - evilGiraffe – honeypotsRus
 - github.com/cowrie/cowrie

37



LAB 1

- Install cowrie <https://github.com/cowrie/cowrie>
- rsync -avzhe ssh honey@192.168.3.112:/ cowrie/honeyfs
 - (did you add a honeytoken?)
- ./bin/createfs -l honeyfs -d 5 -o share/cowrie/ubuntu.pickle

38

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

39

REMEMBER

84%

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

Source: Verizon Data Breach Report, 2014

40

TAKEAWAYS

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

41

THANK YOU!!!

- *Kat Fitzgerald*
 - @rnbwkat
 - evilkat@rnbwmail.com



42

APPENDIX

- Some suggestions for the “Lab”
- Setup a “source” VM such as Ubuntu 14, 16 or 18. Something a little older.
 - Do NOT patch!
- Follow standard Cowrie installation instructions on Debian VM
- The key to customizing – the ./etc/cowrie.cfg
 - The honeypot filesystem is in honeyfs – these files can be Viewed/cat, etc.
 - The files that are visible but can be displayed are in pickle.fs
 - Think about the type of honeypot you want to create. If you want a honeydoc, it must exist in honeyfs, AND in pickle.fs – the difference is, the ones in honeyfs can be accessed as well as listed.

43

APPENDIX - 2

- You will find a lot of configuration options in cowrie.cfg, including all the headers, banners, etc. Take some time to read through it
- There are several other config files related to commands, output and more. A great article is [here](https://cryptax.medium.com/customizing-your-cowrie-honeypot-8542c888ca49) (<https://cryptax.medium.com/customizing-your-cowrie-honeypot-8542c888ca49>), but not the only one – do a little searching to see what else you can find on customizing Cowrie.
- To generate a json output file of PS from your source system, you can use (some usernames are used to exclude from the output – change as needed:

```
ps -eo pcpu,%mem,pid,rss,start_time,stat,bsdtime,tty,user,vsz,args | egrep -v
'^(ps - eo|jq|egrep|awk|wazuh|ossec|dovecot|exim|qemu)' | awk
'{for(i=1;i<=10;i++){printf "%s\t",$i}out=$11; for(i=12;i<=NF;i++) {out=out" "$i};
print out}' | jq -s --slurp --raw-input --raw-output 'split("\n")|[1:-1] |
map(split("\t")) | map(["COMMAND":.[10], "CPU":.[0]|tonumber, "MEM":.[1]|tonumber, "PID":.[2]|tonumber, "RSS":.[3]|tonumber, "START":.[4], "STAT":.[5], "TIME":.[6], "TTY":.[7], "USER":.[8], "VSZ":.[9]|tonumber}) | {
"command": { "ps": .}}'
```

44

MONITORING

WAZUH – SINGLE LINE INSTALL – MAKE SURE THERE IS AT LEAST 250G AND 4G RAM FOR GOOD PERFORMANCE

```
curl -s0 https://packages.wazuh.com/4.4/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```