SWEET DECEPTIONS
THE ART OF CUSTOMIZING HONEYPOTS

Kat Fitzgerald
Staff Security Engineer

@rnbwkat
@rnbwkat@infosec.exchange

evilkat@rnbwmail.com

1

$ whoami

- *CEO @BSidesChicago, 2019 COO @dianainitiative, CFP Lead @BSidesPGH, DefCon 3!*
- *Based in Chicago 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*
- *Pentester!!*

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.
- *Complexity is the Enemy of Security*

3

DISCLAIMER (PART 2)

- I'm obsessed(?) with home security labs and honeypots
- 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 $161 billion - 2022
- 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

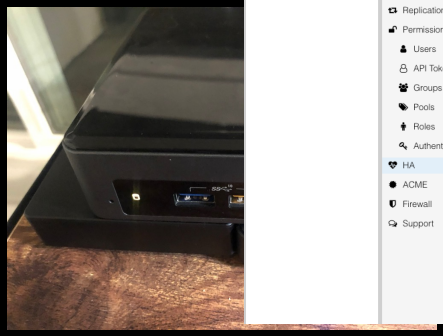
BUT FIRST..

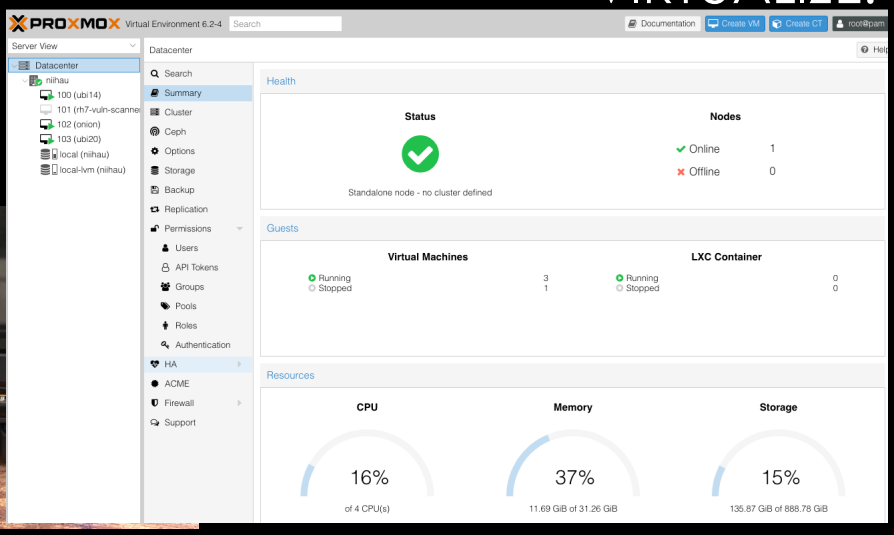
Your Lab!

- Virtualize
  - Proxmox
- PIs
- OpenWRT
- OpnSense

7

VIRTUALIZE!





8

NETWORK

https://openwrt.org/

9

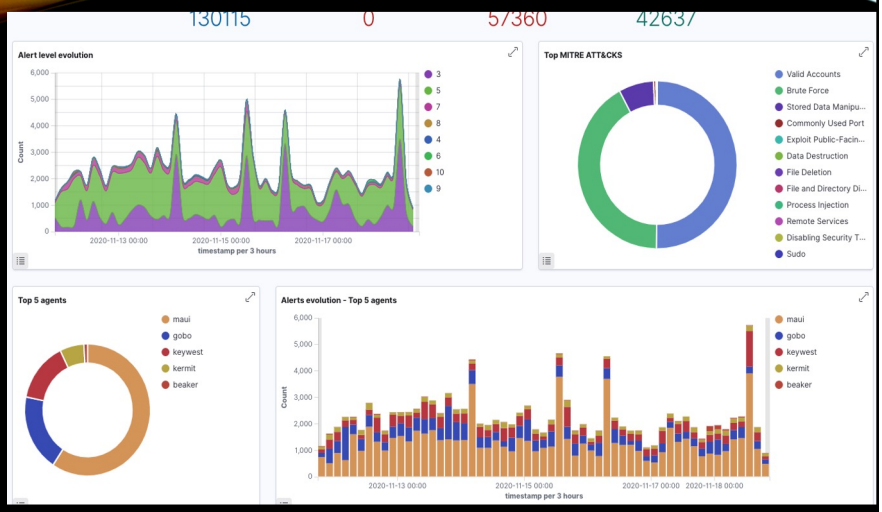
OK – NOW WHAT?

- 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)*
- Monitoring! wazuh.com

10

MONITORING

WAZUH.COM




```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

11

data.eventid	cowrie.login.s
data.message	login attempt
data.password	password
data.sensor	sasha
data.session	d5c6623bdec
data.src_ip	
data.timestamp	2022-08-07T
data.username	root
decoder.name	json
full_log	{"eventid":"co succeeded","
id	1659883190.
input.type	log
location	/home/aladin
manager.name	honeydew
rule.description	root logged ir

Description
raju tried to login to honeypot.
nproc tried to login to honeypot.
root logged into honeypot.
nproc tried to login to honey
root logged into honeypot.
redmin tried to login to hone
Integrity checksum changed
nproc tried to login to honey
root logged into honeypot.
jmjarre tried to login to honeypot.

pinkfloyd tried to login to honeypot.

amministratore tried to login to honeypot.

zimbra tried to login to honeypot.

coinfo tried to login to honeypot.

12

HONEYPOTS

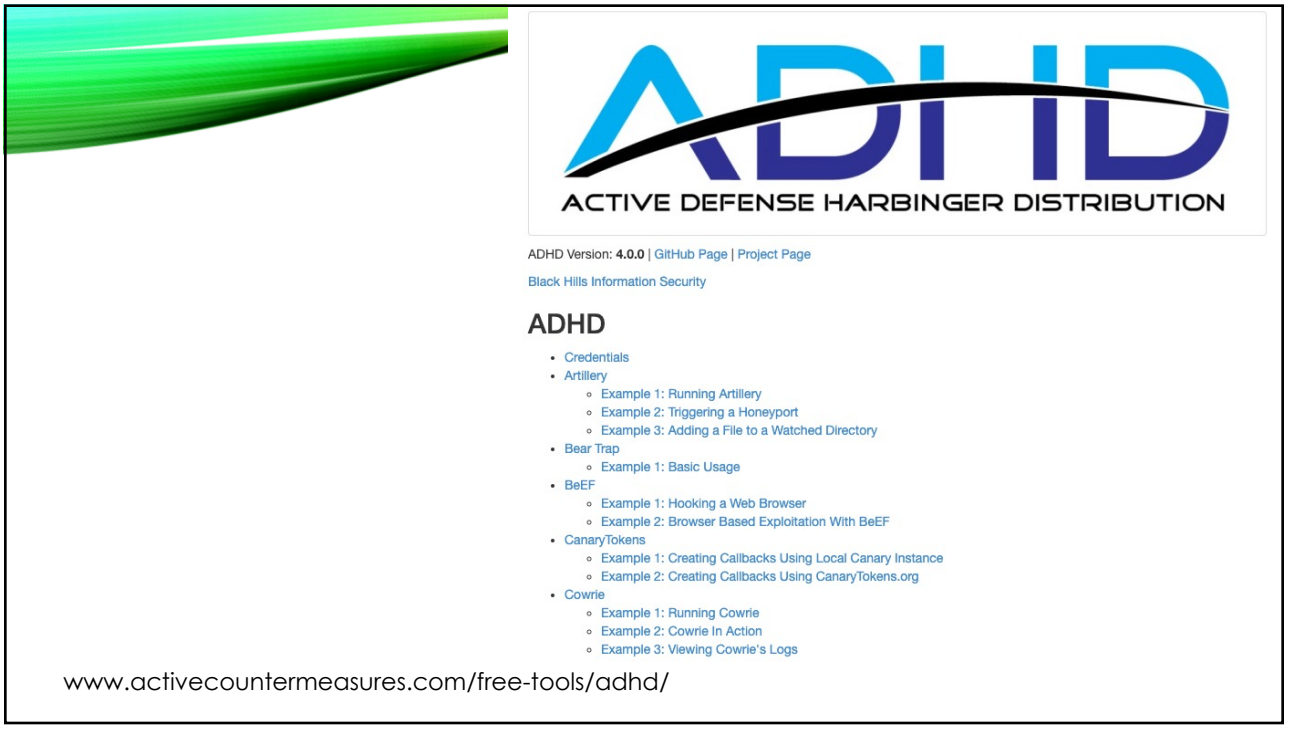
- Honeypots vs Deception
  - A resource with no value(?)
    - Value = Use of Resource
  - Does Not Hack Back
- Important Points
  - Deployment
  - Customization = Planning! (more on this)
  - 100's of "types"

13

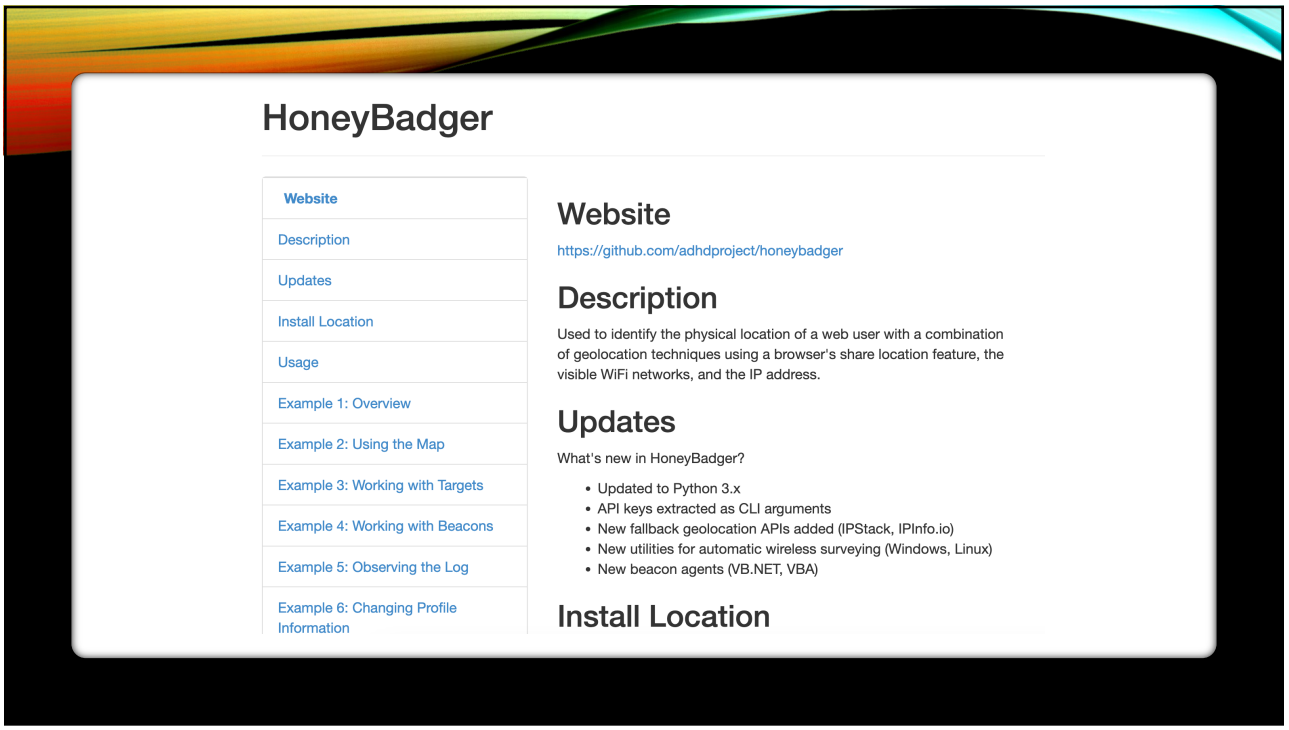
PICK ONE

- OpenCanary -- opencanary.readthedocs.io/en/latest/
- Honey Badger -- github.com/adhdproject/honeybadger
- LLM powered-- github.com/0x4D31/galah
- CHN-- communityhoneynetwork.readthedocs.io/en/stable/
- Canarytokens -- canarytokens.org/generate
- T-pot -- github.com/telekom-security/tpotce
- Cowrie -- github.com/cowrie/cowrie
- Conpot -- github.com/mushorg/conpot
- Lots more -- github.com/paralax/awesome-honeypots
- What about the "Real Thing"? Hmmmm.. (eBPF??)

14


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
www.activecountermeasures.com/free-tools/adhd/

15


HoneyBadger
Website
Description
Updates
Install Location
Usage
Example 1: Overview
Example 2: Using the Map
Example 3: Working with Targets
Example 4: Working with Beacons
Example 5: Observing the Log
Example 6: Changing Profile Information
Website
https://github.com/adhdproject/honeybadger
Description
Used to identify the physical location of a web user with a combination of geolocation techniques using a browser's share location feature, the visible WiFi networks, and the IP address.
Updates
What's new in HoneyBadger?
Updated to Python 3.x
API keys extracted as CLI arguments
New fallback geolocation APIs added (IPStack, IPInfo.io)
New utilities for automatic wireless surveying (Windows, Linux)
New beacon agents (VB.NET, VBA)
Install Location

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 atls
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

OODA VS CCAD

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

19

THE HARD PART - DEPLOYMENT

- Plan, Plan, Plan!
  - Low, Medium
  - Honeypots, Honeyports, Honeytokens, Honeycreds
  - Customization ← *Ding ding ding!*
    - Real vs Self-Signed Certs
    - Actual Applications
  - HIDS Wazuh / SIEM
    - Rules! Tuning
- Where?
  - Server Farms
  - Cloud Storage
  - IoT (Shodan is your friend!!)
    - https://shodan.io
  - DMZ (Guest WiFi)
  - MX, DNS
  - PoS

20

MORE CUSTOMIZATION

- Shodan
  - Banners
  - Versions!
  - HTML
- HoneyTokens
- Hosts
  - Filesystems
    - github.com/referefref/honeyfs
  - Commands
  - History
  - Processes
  - HoneyTokens

Real Servers and Apps
- Staging

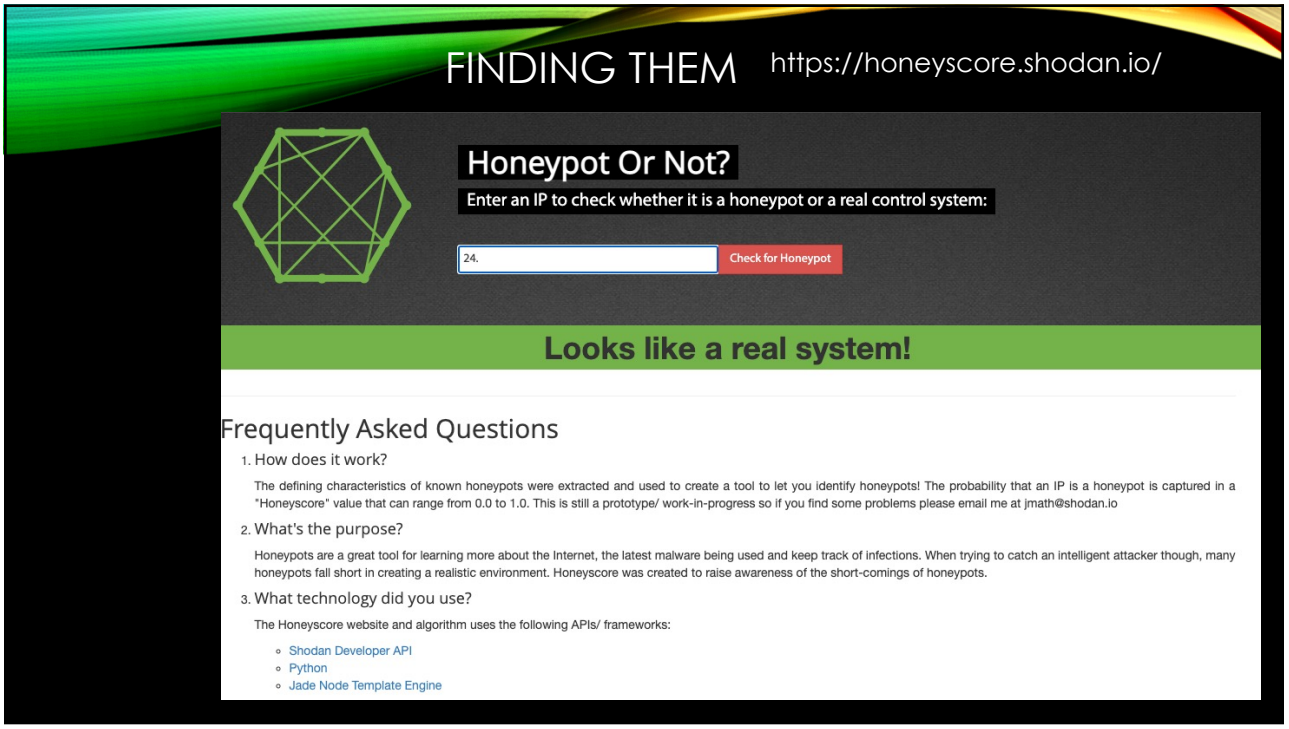
Too legit to quit!!
Make it look real!

21

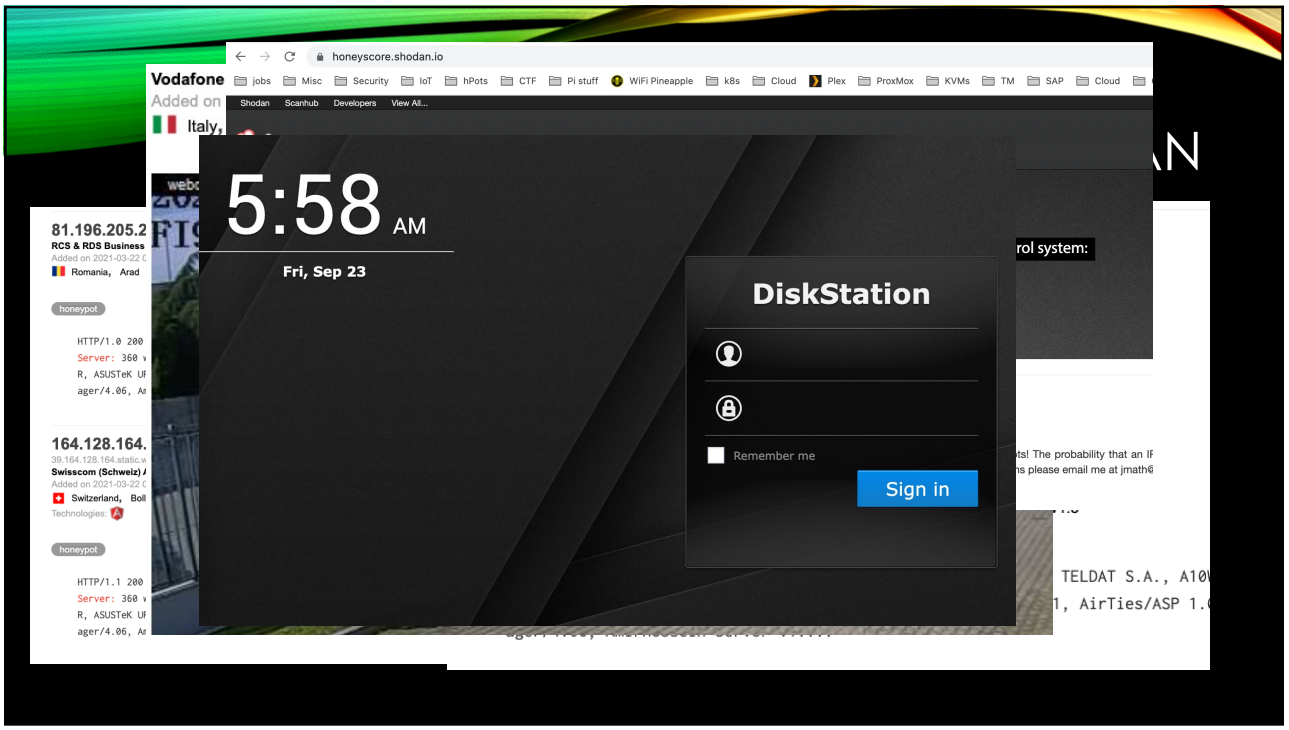
- An Idea

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

22


FINDING THEM
https://honeyscore.shodan.io/
Honeypot Or Not?
Enter an IP to check whether it is a honeypot or a real control system:
24.
Check for Honeypot
Looks like a real system!
Frequently Asked Questions
1. 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 is a honeypot is captured in 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 jmath@shodan.io
2. What's the purpose?
Honeypots are a great tool for learning more about the Internet, the latest malware being used and keep track of infections. When trying to catch an intelligent attacker though, many honeypots fall short in creating a realistic environment. Honeyscore was created to raise awareness of the short-comings of honeypots.
3. What technology did you use?
The Honeyscore website and algorithm uses the following APIs/ frameworks:
Shodan Developer API
Python
Jade Node Template Engine

23


honeyscore.shodan.io
Vodafone
Added on
Italy,
5:58 AM
Fri, Sep 23
DiskStation
Remember me
Sign in
81.196.205.2
RCS & RDS Business
Romania, Arad
honeypot
164.128.164.
Swisscom (Schweiz)
Switzerland,
honeypot
TELDAT S.A., A10
AirTies/ASP 1.

24

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
```

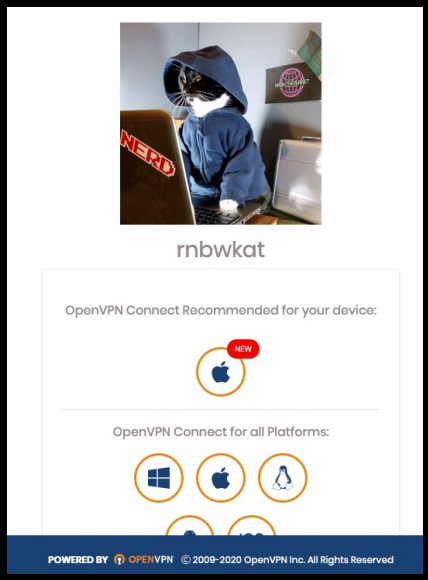
25

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
```

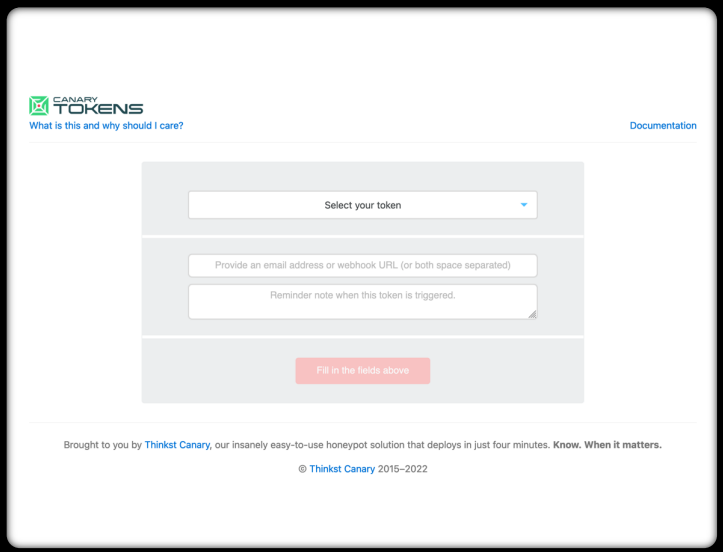
26

WHAT IS IT?



27

- https://www.canarytokens.org/generate



28

MORE CUSTOMIZATION

Cowrie

- The obvious
  - Hostname (and MAC!)
    - `openssl rand -hex 6 | sed 's/\(..\)/\1:/g; s/:$//'`
    - `00:11:32:B3:4D:F5`
  - Versions
  - History
  - Commands
    - History -s (or just copy .bash_history)
    - Targets?
  - Filesystem
  - Processes
  - Usernames
    - Honeycreds

29

SSH/TELNET CUSTOMIZATION

- Banners = easy, but don't forget ssh headers/ciphers/version
- Ping?
- DNS?
- rsync is your friend
- ps a running system
  - 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 15525  4868 Feb04 Ss     6:14 ?        root     279644 php-fpm: master process
 0.0  0.0 15533  6816 Feb04 S      0:00 ?        emps     280408 php-fpm: pool ordinary
```

30

CUSTOMIZATION EXAMPLES (CONT)

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

31

KEY TAKEAWAYS

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

github/rnbwkat/presents/honeypots_2024.pdf

32

THANK YOU

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

33