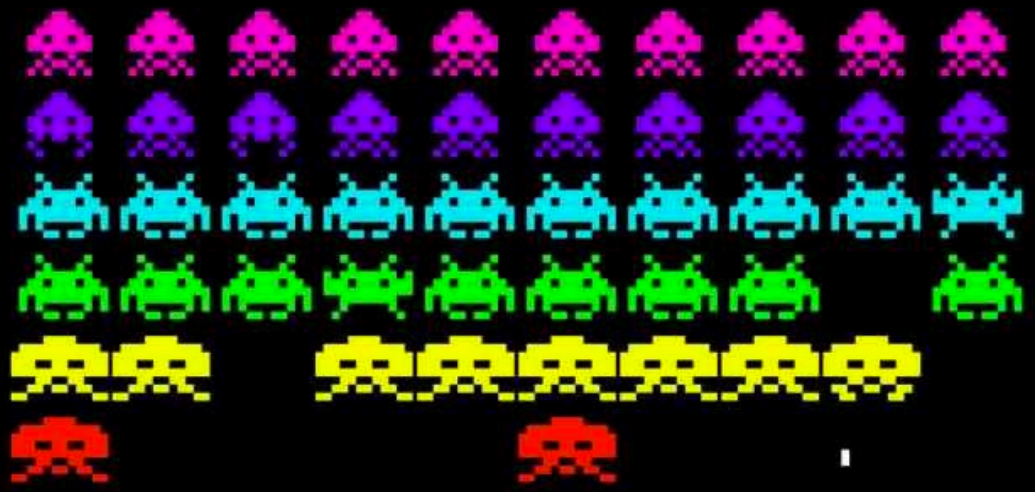


ALL YOUR IOT ARE BELONG TO *ME*

Yolonda N. Smith
Director of Product Management, Pwnie Express

Prepared for Adobe DEFENDCON, 21 September 2017

"Ok, so I mixed my memes.
Give me a break"

– Old English Proverb

Prepared for Adobe DEFENDCON, 21 September 2017

OVERVIEW

- Housekeeping
- About Me
- A Typical IoT Ecosystem
- A Brief Recap on Ways to Deal with Risk
- Defensive Techniques in IoT
- All Your IoT Belongs to *Me:* A Demonstration
- Strategy, Operations and Tactics to Deal with the IoT Island
- Questions

Prepared for Adobe DEFENDCON, 21 September 2017

ABOUT ME

- Then: USAF Cyber Defense Operations Officer
- Iraq, Afghanistan,Djibouti deployments
- Advanced Network Operations + NSA
- AF cyber defense capabilities development
- Now: Director of Product Management, Pwnie Express
- Focused on closing the IoT Security Gap
- Discovery, classification, correlation & prevention of business disruption caused by proliferation of IoT systems

Prepared for Adobe DEFENDCON, 21 September 2017

ABOUT ME

- Sometimes:
  - Ameture beer brewer
  - Animal rescue
- Always:
  - Focused on getting (and keeping) girls/women involved in STEM
  - Mentorship: Black Girls Code
  - National Society of Black Engineers Professional Development

WHY ARE WE HERE TODAY?

...ony on Sunday. A10

...RATES
...WORK

...rry in the West
...gested it would be able

Global Hack Pressures Officials, Victims

Security experts ... of new threats ... investigators be... hunt for perpetr...

The cyberattack th... around the globe ... weekend, hitting bu... hospitals and gov... agencies in at least 1... tries, is likely to keep growing as people around t... turn to work, law... authorities warned.

By Nick Ko... Jenny Gross and Stu ...

Investigators ... far-reaching hunt ... petrator, as ... around the world ... mitigate damage from the highest-profile computer-worm outbreak in nearly a decade. Europe's police coordination agency estimates 200,000 individual terminals had fallen victim ... while Chinese authorities ... the number as high ... lion world-wide.

"This is something we have ... ven't seen before," Europol di...

"Everyone was running around saying we've been hacked…it spread like wildfire"

Mohamed Amri
Parts Maker, Renault SA France

21 Hacked Cameras, D... Massive Internet Ou...

OCT 16

...services in the aftermath of the attack.

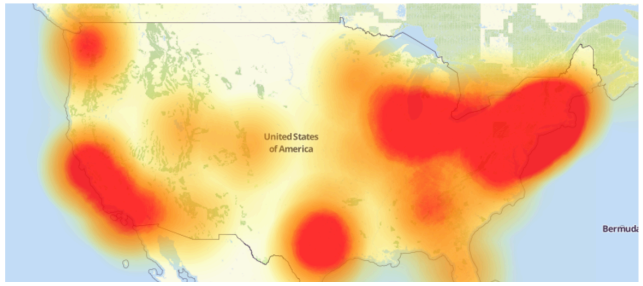
Dyn Customer Analysis: Before and After Mirai DDoS Attack

The data analyzed a representative sample of 178,000 domains hosted on Dyn before and immediately after the 2016 attacks, and revealed that more than 14,000 internet domains dropped Dyn as their DNS service provider in the wake of the incident (roughly 8%).

The findings are interesting because it's rare that the financial fallout from a DDoS attack is laid out so clearly in the public eye. But when you consider the impact of the attack on Dyn's ...

...net a ...per of Web sites was launched with the help of hacked ... such as CCTV video cameras and digital video recorders,

...an training their attack cannons on **Dyn**, an Internet ...des critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

The direct costs of computer downtime from the cyberattacks totals around $8 billion

The RISK Team provided me with a report detailing known indicators found in the firewall and DNS logs that I had sent over earlier. Of the thousands of domains requested, only 15 distinct IP addresses were returned. Four of these IP addresses and close to 100 of the domains appeared in recent indicator lists for an emergent IoT botnet. This botnet spread from device to device by brute-forcing default and weak passwords. Once the password w... known, the malware had full control of the device a... would check in with command infrastructure for up... and change the device's password – locking us out ... 5,000 systems.

While we waited for the full packet capture solution to be set up, I instructed the Network Operations Team to prepare to shut down all network access for our IoT segments once we had intercepted the malware password. Short lived as it was, the impact from severing all of our IoT devices from the internet during that brief period was noticeable across the campus – and we were determined never to have a repeat incident.

"Short of replacing every soda machine and lamp post, I was at a loss for how to remediate the situation"

Incident Commander
Unnamed Canadian University

TYPICAL IOT ECOSYSTEM

- Device 
- Gateway 
- Connectivity 


Secure Upgrade Pathing + Patching

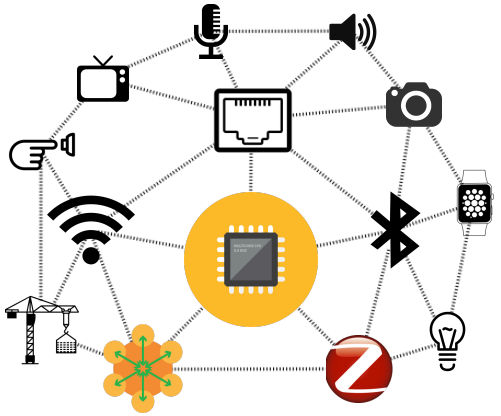

Secure Configuration


Concept of ‘System’

Prepared for Adobe DEFENDCON, 21 September 2017

WHAT MAKES IOT SO SPECIAL?

1. Multiple communications paths on a single chip
2. Direct and demonstrable impact on physical world
    1. Health, safety & life support systems
    2. Drives critical systems which run key business & P/L initiatives
3. Machine longevity & security mismatch
4. Value placed on rush to market instead of security



QUICK RECAP: RISK CONTROL STRATEGIES

1. Ignore it
2. Defer it
3. Isolate it
4. Accept it (usually with conditions)

"I don't have a problem with IoT. If people need a webcam or something, I'll just put it on a separate network segment. They can deal with the consequences."

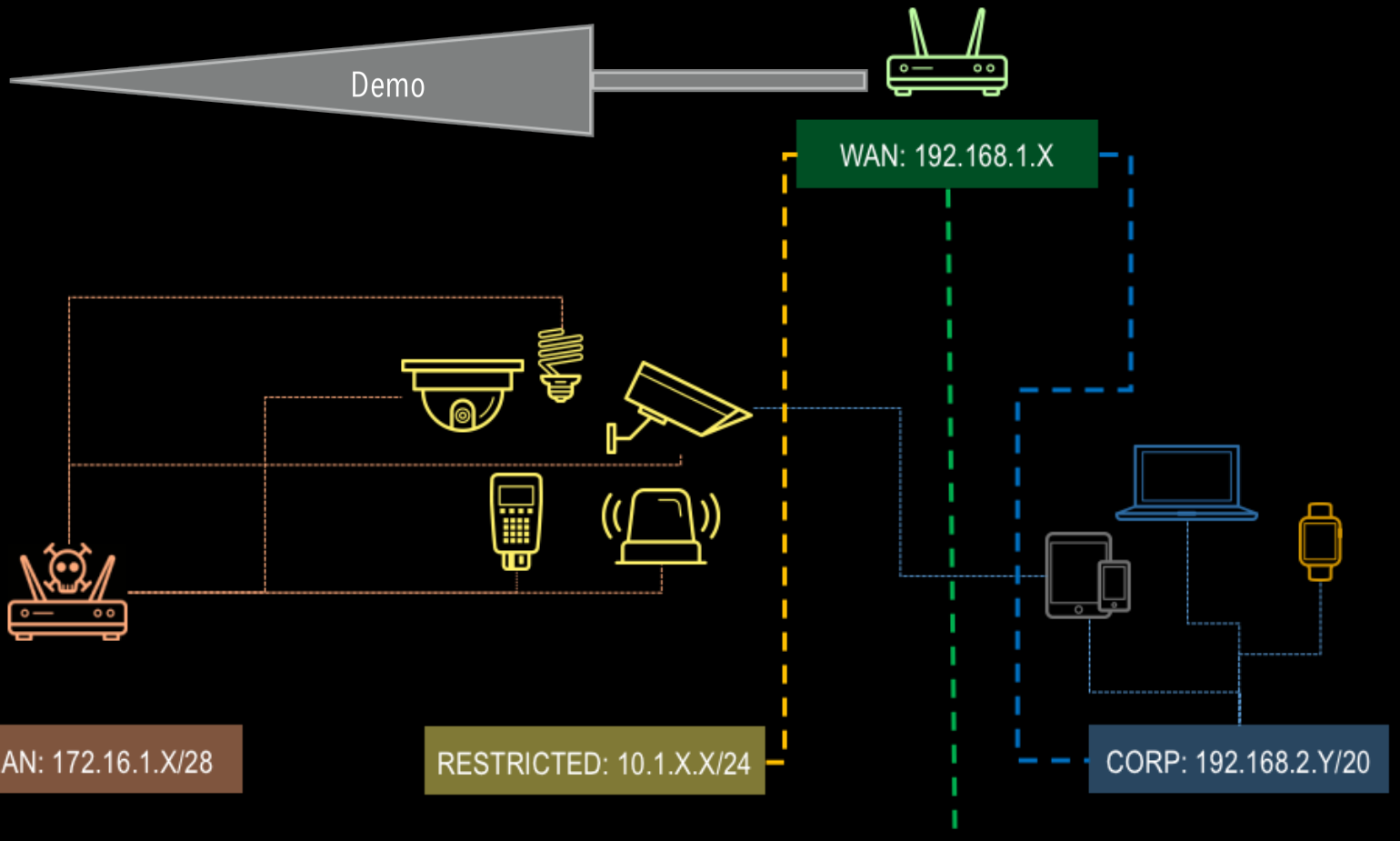
– Actual CISO of a New York University Healthcare System

Prepared for Adobe DEFENDCON, 21 September 2017

COMMON DEFENSIVE STRATEGIES

- Don't allow it on the network
- Isolate it to a different network (airgap)
- VLAN + Network Segmentation
- Willful ignorance/didn't know it was there

CONCEPT OF OPERATIONS



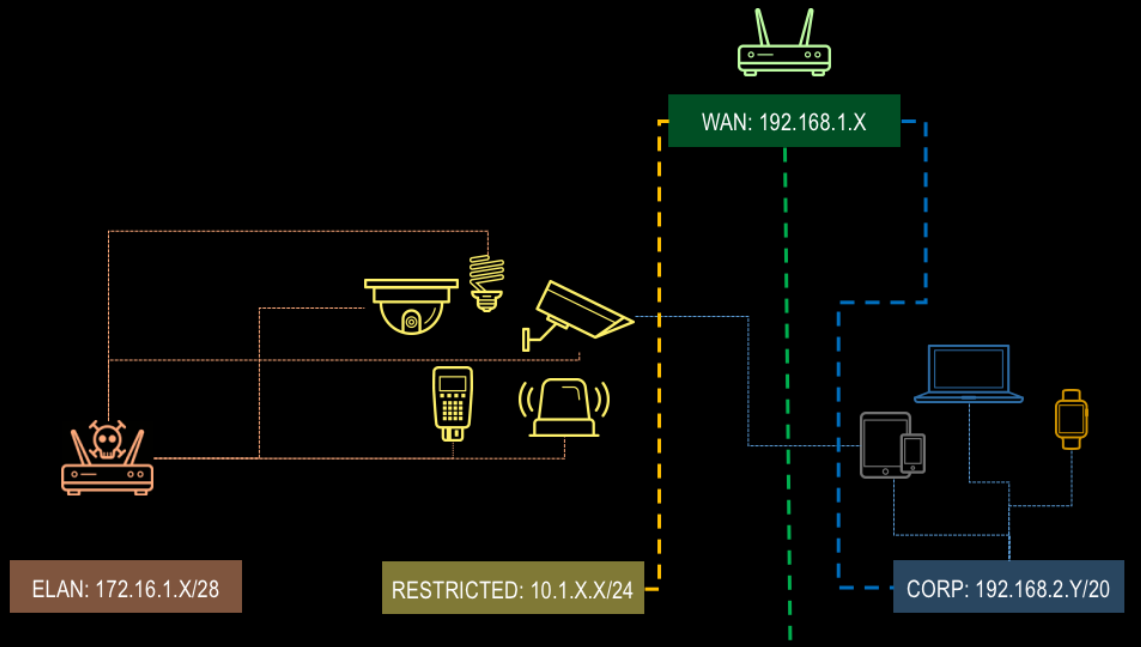
Prepared for Adobe DEFENDCON, 21 September 2017

DEMONSTRATION

Prepared for Adobe DEFENDCON, 21 September 2017

CONSTRUCTING THE ATTACK

1. Steal the network (and keep it)
2. Port/service scan
3. Plant malware
4. Embed a backdoor
5. Hack the planet



Prepared for Adobe DEFENDCON, 21 September 2017

TOOLS REQUIRED

1. Hak5 Pineapple running evil AP
2. Ubuntu Linux VM
   - Fing network scanner (port/service fingerprinting)
   - Python & Ruby scripts (malware development)
   - Netcat (backdoor placement)
3. CWIPS to keep everything under my control

Total cost for this attack: $150 USD

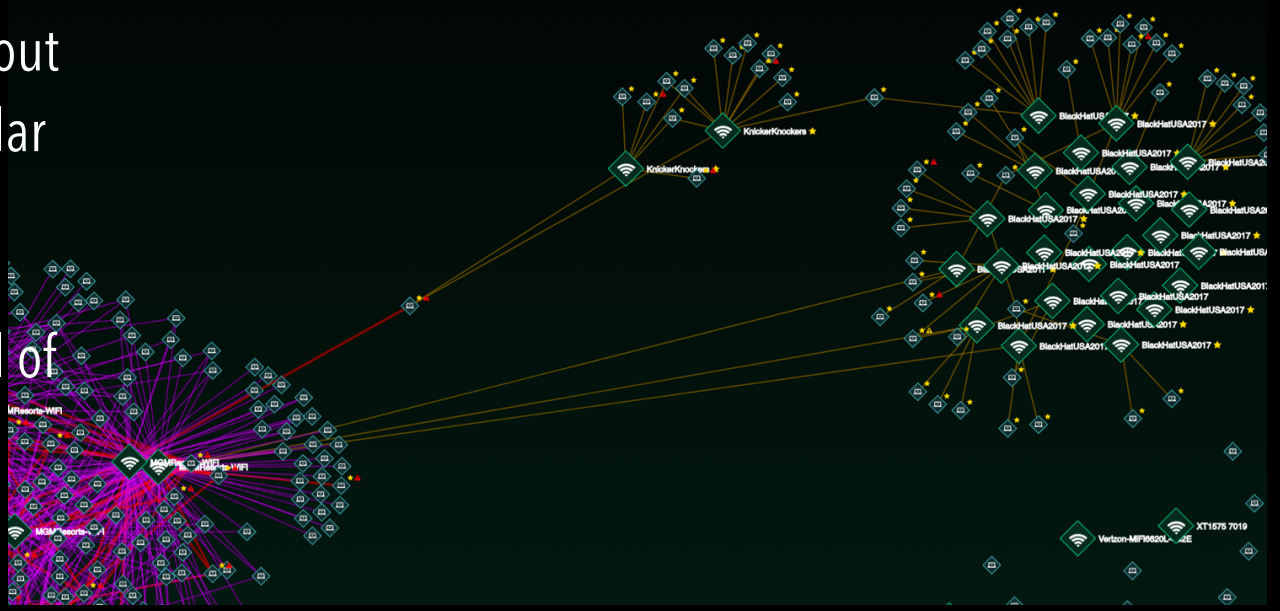
WHAT YOU WON'T SEE

Cracking of WPA passwords

- If you want info on that, check out aircrack-ng, coWPAtty and similar tools

The epic battle raging for control of the devices

- Devices are dumb & Wi-Fi is ubiquitous



This demonstration was prepared with the expressed and written permission of the DefendCon Conference team and the hosting organization, Adobe. The demonstration was tested and vetted on specific devices, networks and software. As a precaution, now would be a good time to turn off your Wi-Fi. If you leave it on and your devices stop working, I'm going to make this face: 😫 followed immediately by this face ¯_(ツ)_/¯

DISCLAIMER

"But isn't this just consumer IoT?"

Prepared for Adobe DEFENDCON, 21 September 2017

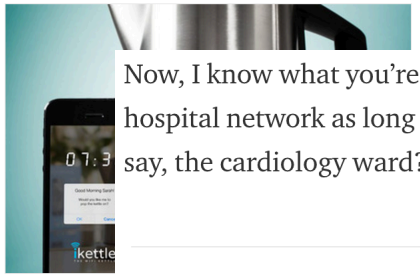
REAL WORLD EXAMPLE

Security

Connected kettles boil over, spill Wi-Fi passwords over London

Pen-tester's killer cuppas made in cracked iKettle

By Darren Pauli 19 Oct 2015 at 05:57 124 SHARE ▼



A security man has ma
across London, provin

Now, I know what you're thinking: *who cares* if the smart kettle ends up on th
hospital network as long as it's not on a super-special network segment like,
say, the cardiology ward? Well, I don't want to burst your bubble:

23 2000

Services

23
tcp
telnet

[redacted] Cardiology [redacted]

user:

2000
tcp
ikettle

\xff\xfb\x01\xff\xfb\x03\xff\xfd\x18\r\[redacted] Cardiology [redacted]\r\n\n\n\ruser:

Yolonda Smith
May 30 · 7 min read

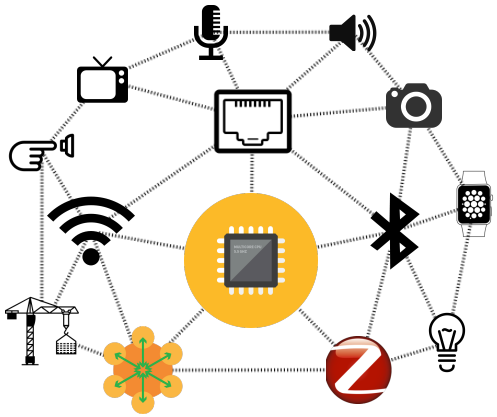
How Your Doctor's Coffee Jones is Going to Get Your Personal Data Stolen*

Read more...

NEXT STEPS

Prepared for Adobe DEFENDCON, 21 September 2017

MITIGATING IOT RISK

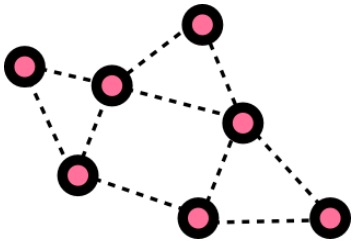


WHOLE DEVICE
PICTURE

1

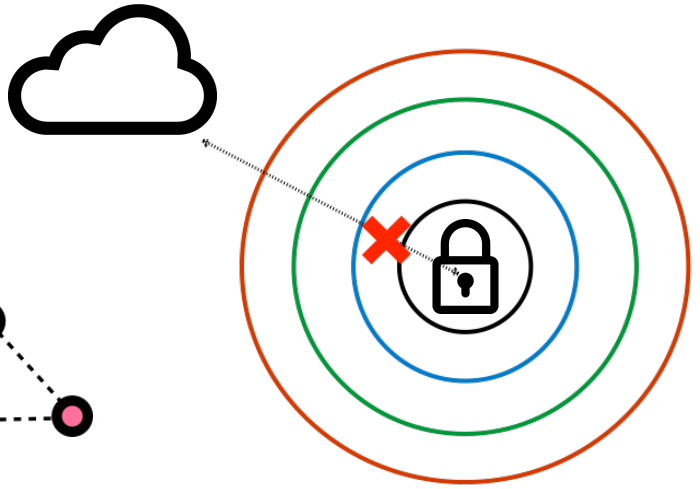
CONTINUOUS
POSTURE ASSESSMENT

2



DEVICE RELATIONSHIP
& SYSTEM CONTEXT

3



FACILITATE
TRUST-DRIVEN ACCESS

4

Prepared for Adobe DEFENDCON, 21 September 2017

GETTING IOT *OFF* THE ISLAND

STRATEGIC

- Starts with acceptance of IoT as yours to know and manage
- Ask about upgrade pathing, resilliency && warranty
- Level of security should match the life expectancy of the system (not just the device)
- Policy must be enforceable && tied to organizational needs

OPERATIONAL

- Network segmentation isn't bad —blind isolation is bad
- IoT: short bursts of communication between long periods of sleep. Your whole stack needs to work together to catch anomalies
- Make sure threat models, TTXs and DFIR drills include IoT scenarios
- Reflect the system & it's long-term importance to the organization

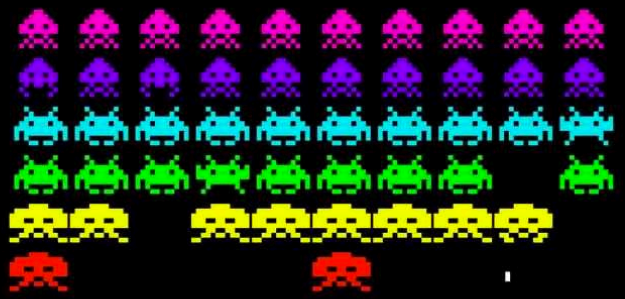
TACTICAL

- Low-hanging fruit: Telnet (TCP 23), FTP (TCP 21), Web Servers (not just on 80)
  - Don't forget UDP!!
- IoT likes 4 protocols:
  - IP
  - Wi-Fi
  - Bluetooth LE
  - Cellular

RESOURCES & ACKNOWLEDGEMENTS

- https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
- https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html
- http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf
- https://medium.com/@ysmithnd/how-your-doctors-coffee-jones-is-going-to-get-your-personal-data-stolen-6cc944d5d92e

- Lisa Lee
- Tracie Martin
- Adobe
- My chiropractor
- Zero_Chaos (Rick Farina)

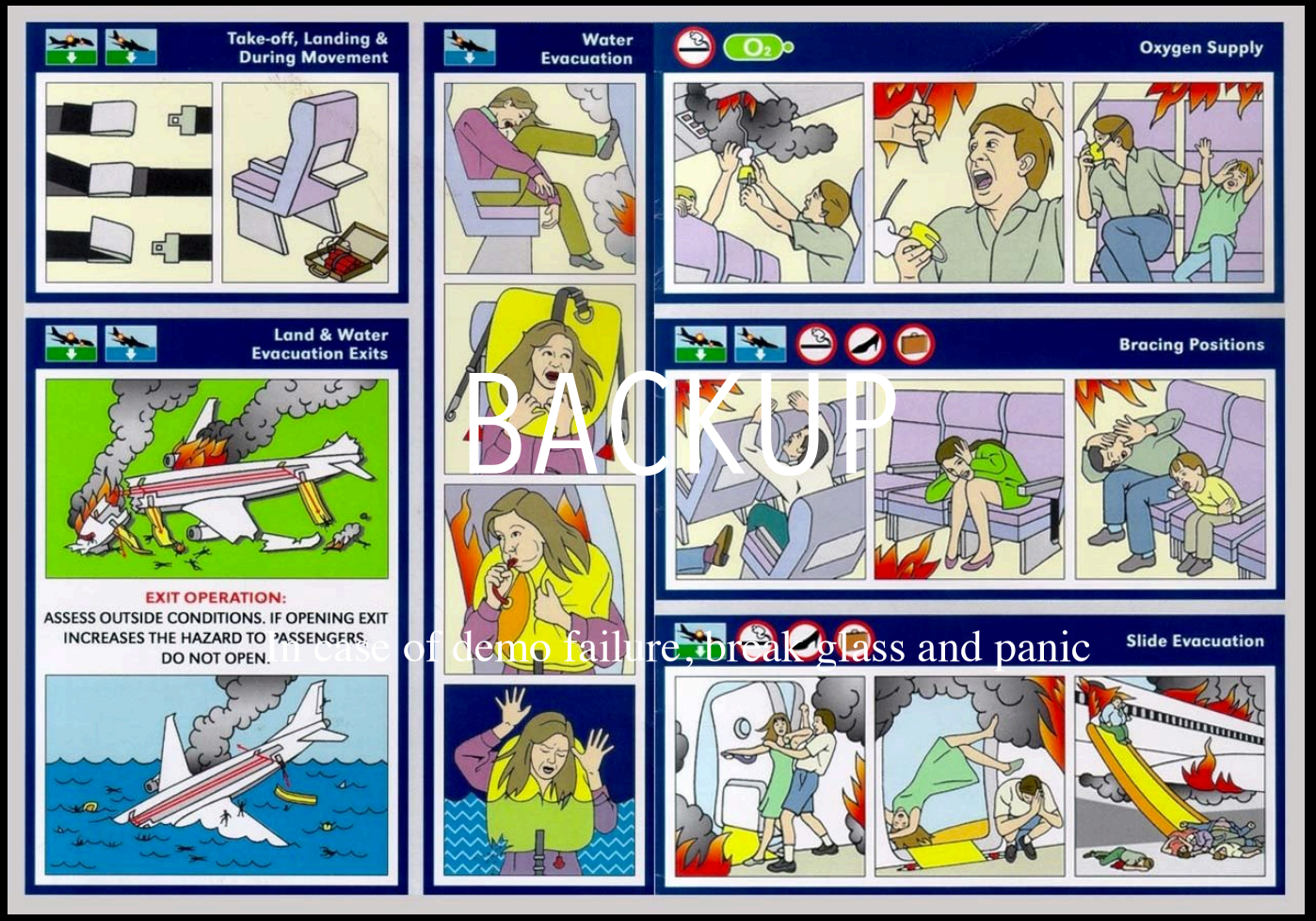


QUESTIONS?

Yolonda N. Smith
Director of Product Management, Pwnie Express

@ysmithND | linkedin.com/in/yolonda-smith | ysmithND@gmail.com

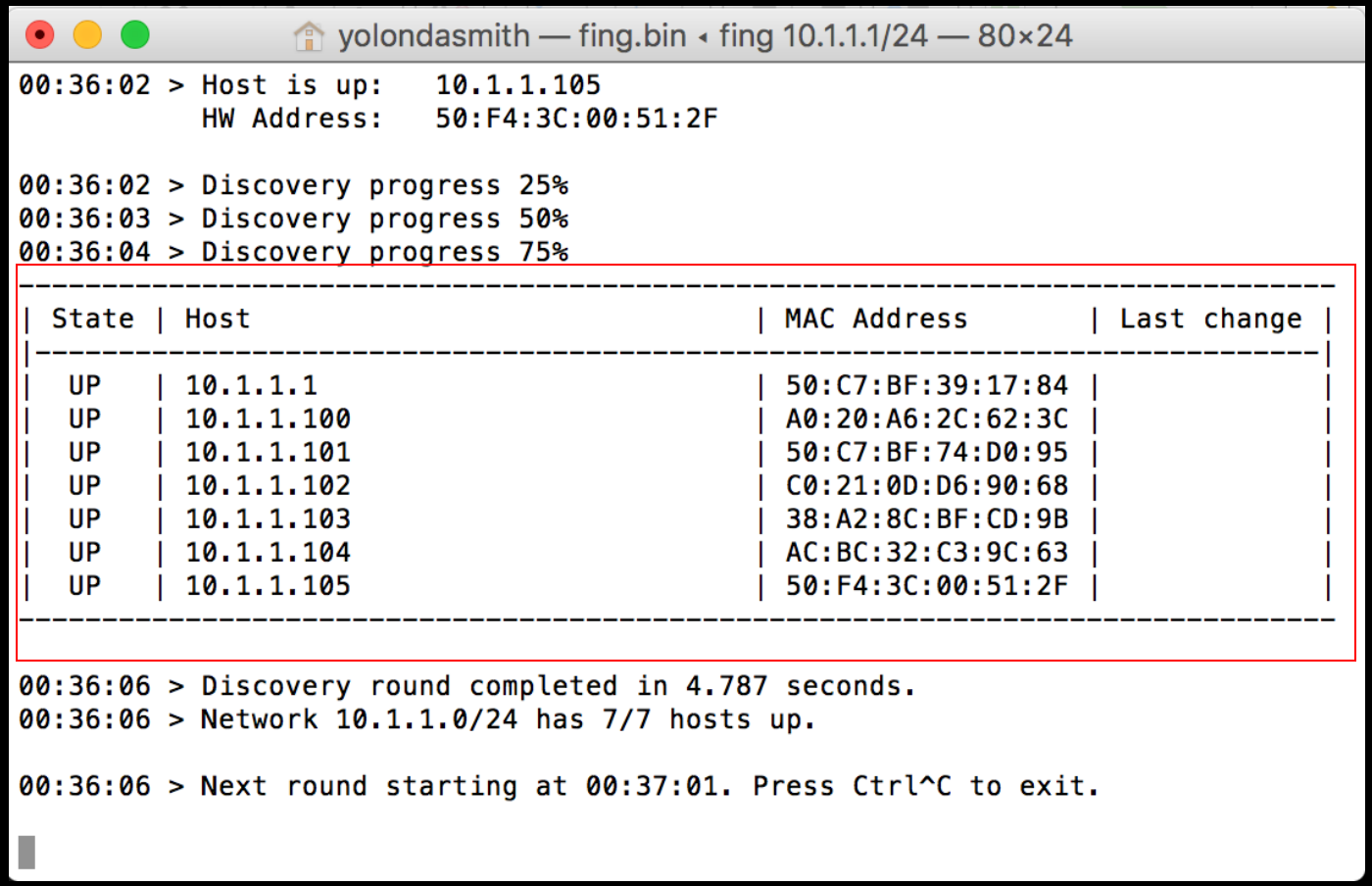
Prepared for Adobe DEFENDCON, 21 September 2017



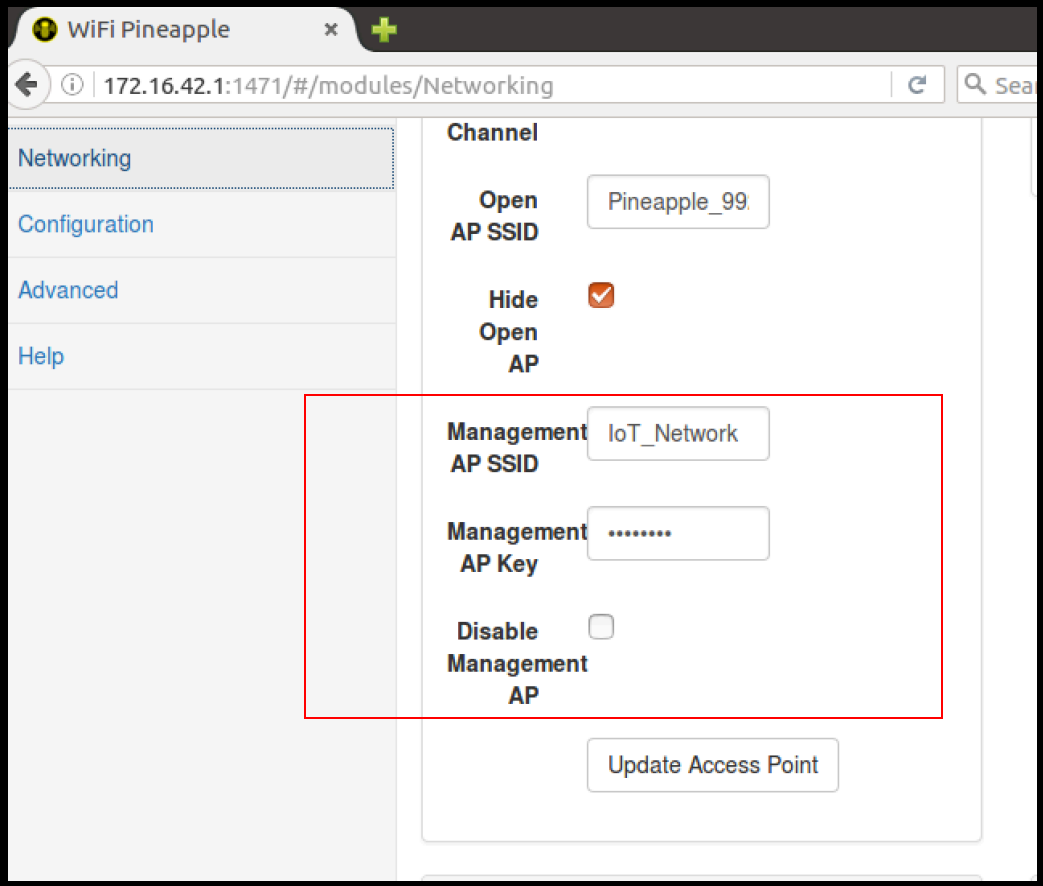
BACKUP

In case of demo failure, break glass and panic

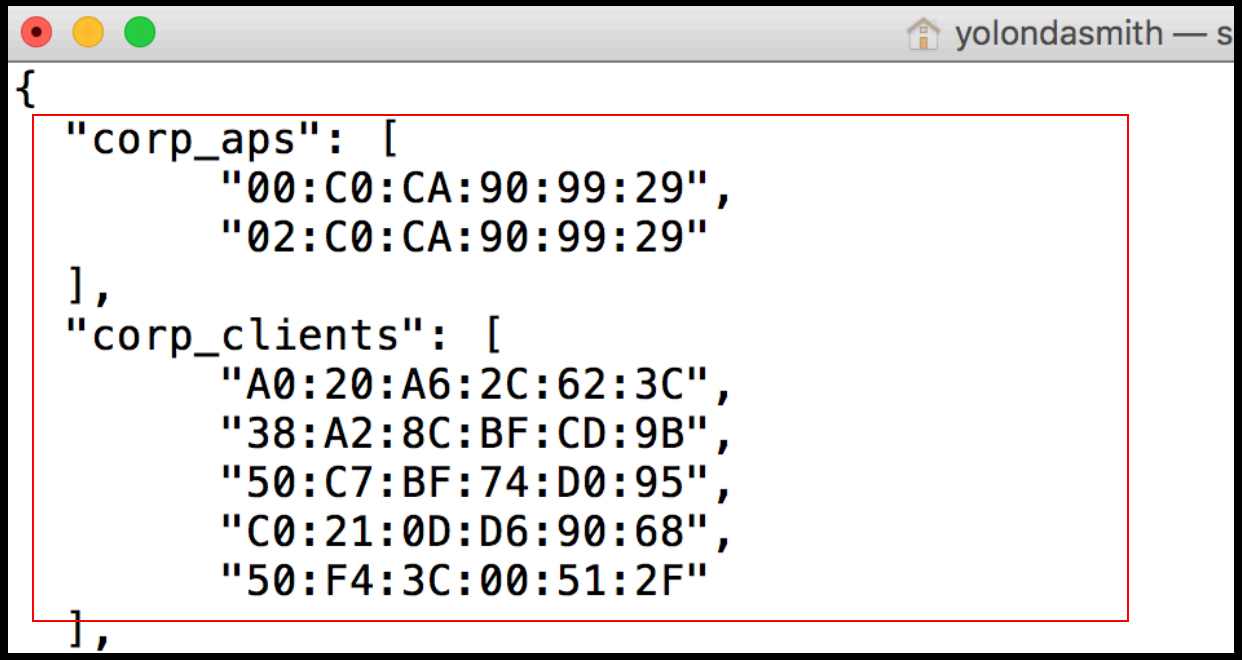
PROOF POINT 1



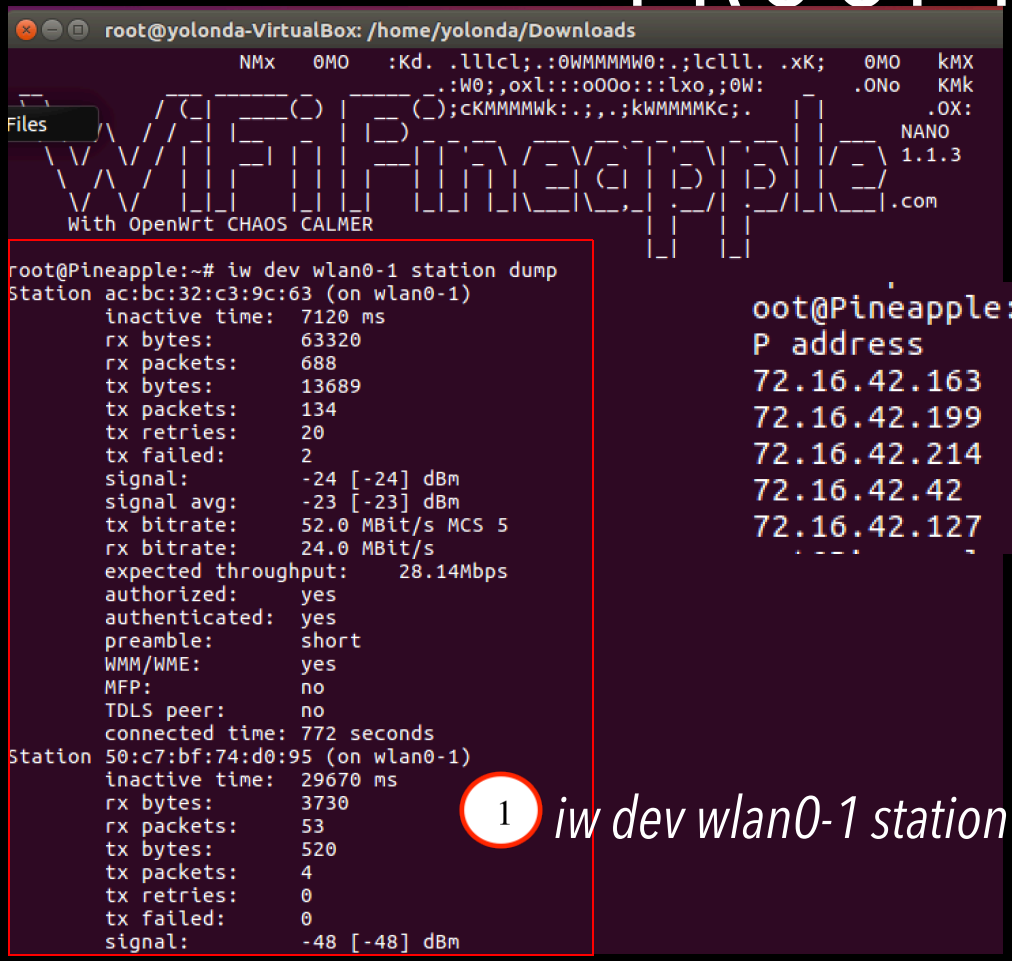
PROOF POINT 2



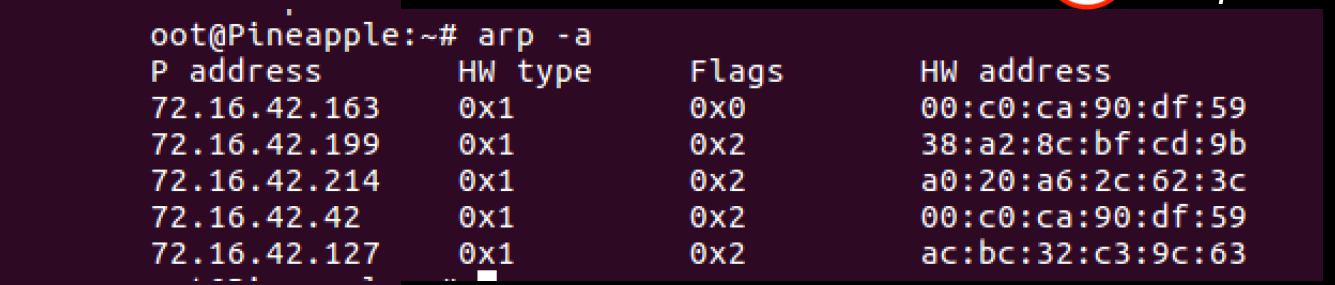
PROOF POINT 3



PROOF POINT 4



1 *iw dev wlan0-1 station dump*



2 *arp -a*

PROOF POINT 5

HotelAndra	2C:5D:93:06:15:A8	Open	no	3	-84
	6C:72:E7:D1:30:77				
HotelAndra	2C:5D:93:06:55:28	Open	no	6	-85
HotelAndra	2C:5D:93:06:6A:F8	Open	no	11	-67
Paxton	30:B5:C2:BE:01:99	Mixed WPA	yes	11	-85
HotelAndra	34:8F:27:27:15:A8	Open	no	3	-82
IoT_Network	50:C7:BF:39:17:84	Mixed WPA	yes	10	-53
CenturyLink5053	58:8B:F3:E5:67:FB	Mixed WPA	yes	11	-90
Wuhoo	60:E3:27:39:C4:35	WPA2	yes	11	-87
Blastworks AirPort01	64:A5:C3:68:74:A8	WPA2	no	6	-90
Pavia System - Wireless	74:3E:2B:11:48:98	WPA2	no	8	-83
SPRW	80:2A:A8:81:EE:64	Mixed WPA	no	6	-91
The Dark Side	8E:15:44:A8:DA:2C	Mixed WPA	no	1	-81
The Dark Side	8E:15:44:A8:DB:87	Mixed WPA	no	11	-80
TDGUEST	94:B4:0F:3C:E5:A0	Open	no	1	-76

PROOF POINT 6

```
172.16.42.127    0x1          0x2          ac:bc:32:c3:9c:
root@Pineapple:~# nc -z -v 172.16.42.199
Error: No ports specified for connection
root@Pineapple:~# nc -z -v 172.16.42.199 1-10000
172.16.42.199 4444 open
172.16.42.199 8000 open
root@Pineapple:~#
```

1 *Kerberos ticketing && webserver*

```
computer    oot@yolonda-VirtualBox: /home/yolonda/Downloads
root@Pineapple:~# nc -z -v 172.16.42.214 1-10000
172.16.42.214 6668 open
root@Pineapple:~#
```

2 *irc*