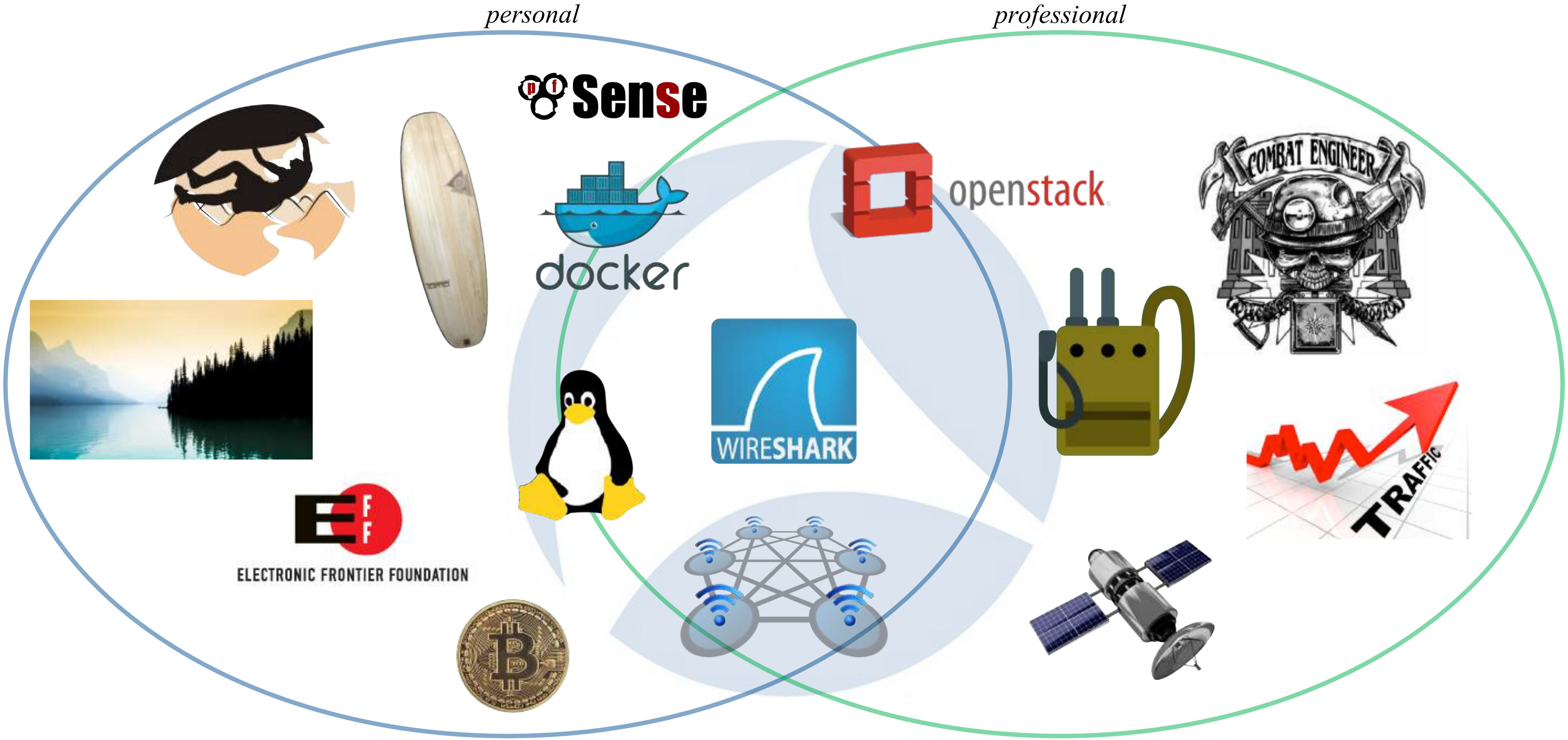
Work Shmerk / Mirai Shmirai:

What are Those Evil Little IoT Devices Doing & How Can You Control Them?

Brad Palm
Lead Network Analyst | BruteForce

Introduction



personal

professional

Itinerary

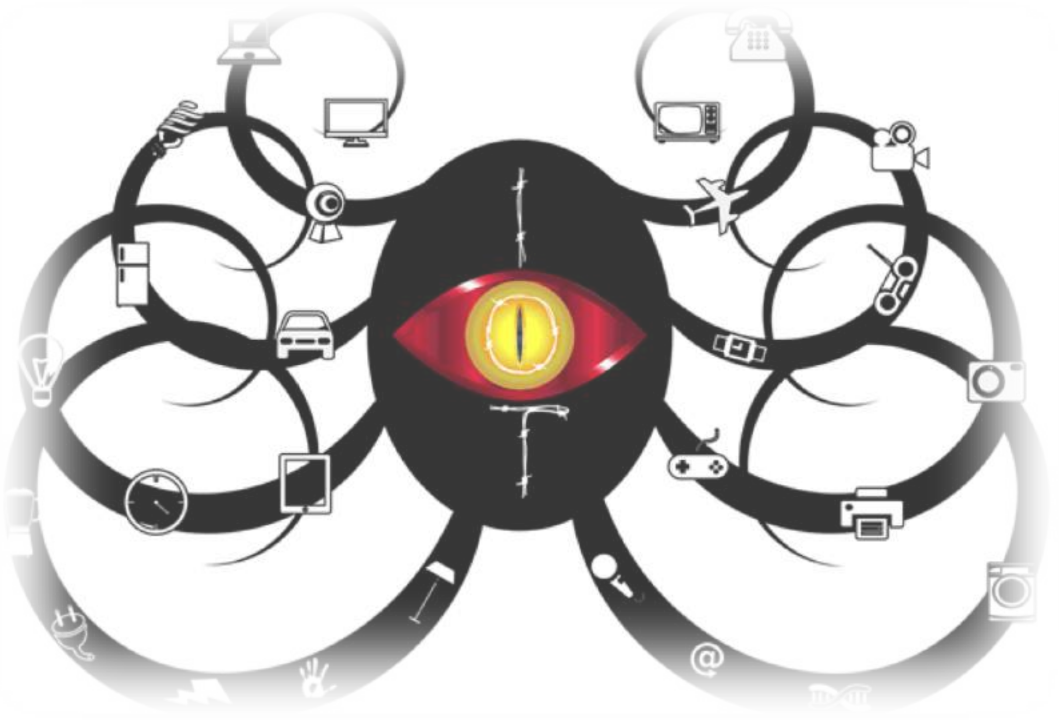
- Goal
- Background
  - IoT
  - Mirai
  - IOCs
  - Motivation
- Own Your Network
  - Brilliance in the Basics
  - Objective
  - Packing List
  - Actions
  - Controls
- Pwn Your Network
  - Why Do I Want to Switch Hats?
  - Reconnaissance
  - Vulnerability/Exploit
  - Scapy
- Lab
  - Scenario
  - ROE
  - Network Diagram
  - Resources

BACKGROUND

Internet of Things (IoT)

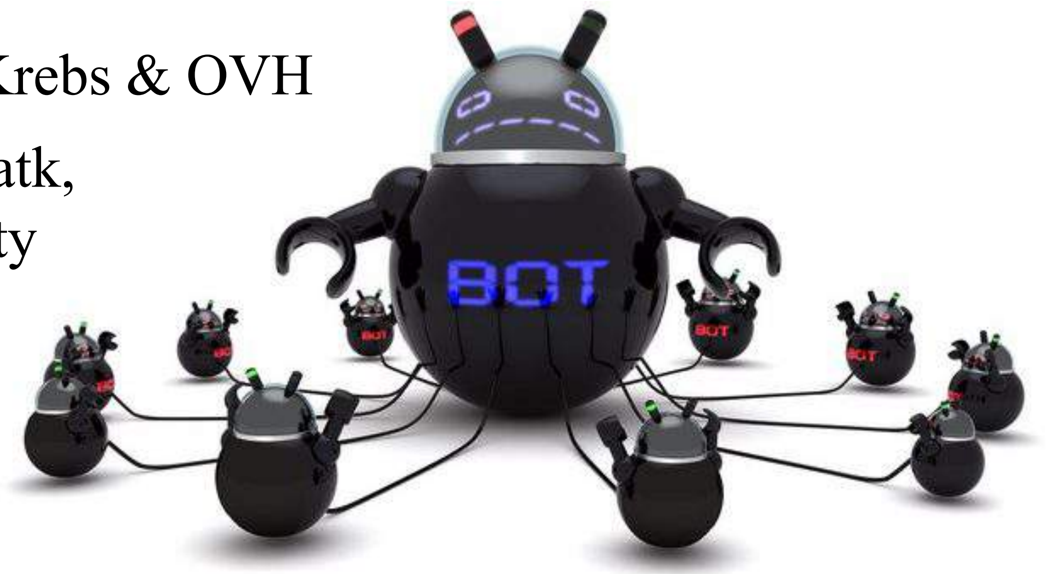
- Running critical systems
- Unseen and unmanaged
- Being shipped insecure by default and will remain so
- Network stressers or booters == mercenaries
- Malware activity more than doubled 2016 #'s
- Gartner projects 20.8 B connected things by 2020

What are these evil little things doing?

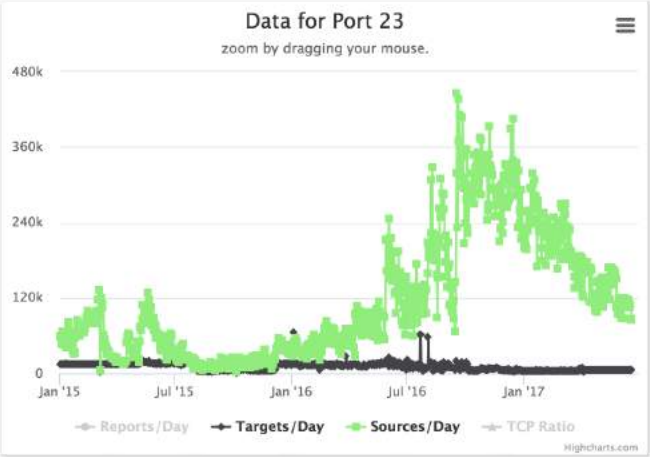


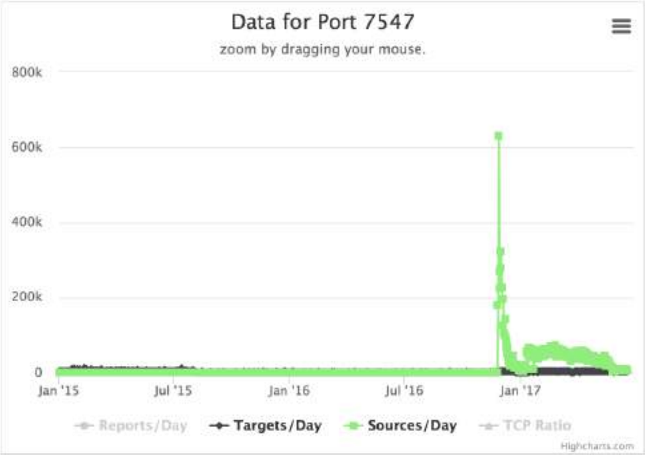
Mirai

- Botnet of connected things – IP cameras, DVRs, routers/modems
- Mirai scans Internet, tries default creds, before exploiting and forcing device to join botnet
- Warmup: 620+ Gbps aimed @ Krebs & OVH
- ~100,000 nodes involved in the atk,
this is a fraction of actual capability
- Game day: ~1Tbps DDOS
brought down Dyn



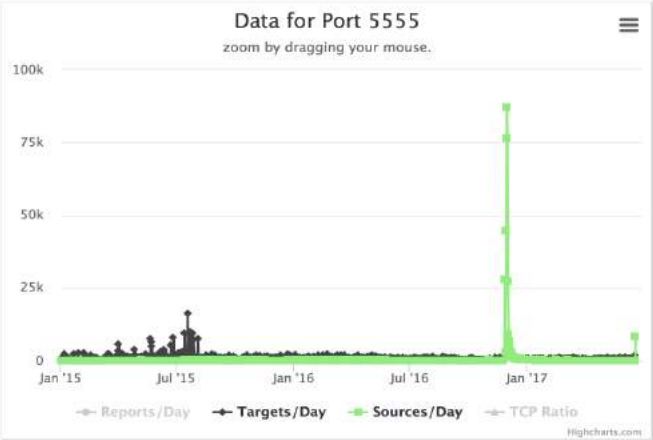
Indicators of Compromise (IOC)

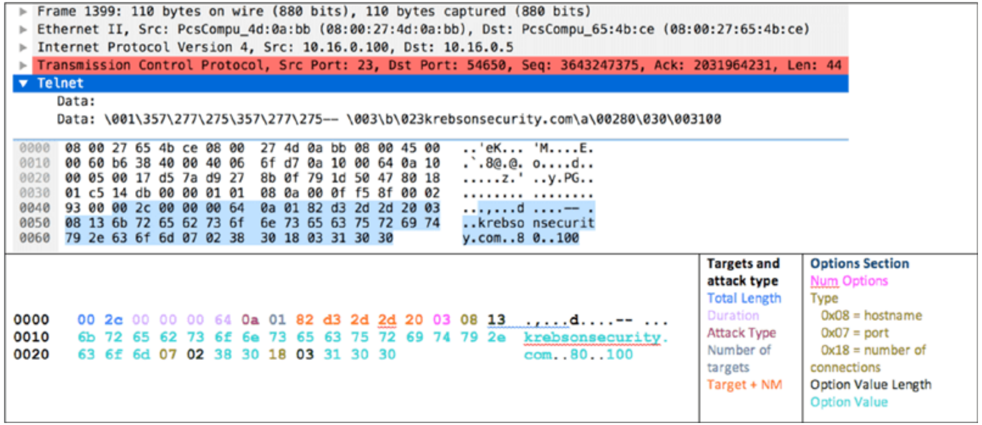




SANS Internet Storm Center Attack Graphs

Ixia Blog – Mirai: A Botnet of Things





```
▶ Frame 1399: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▶ Ethernet II, Src: PcsCompu_4d:0a:bb (08:00:27:4d:0a:bb), Dst: PcsCompu_65:4b:ce (08:00:27:65:4b:ce)
▶ Internet Protocol Version 4, Src: 10.16.0.100, Dst: 10.16.0.5
▶ Transmission Control Protocol, Src Port: 23, Dst Port: 54650, Seq: 3643247375, Ack: 2031964231, Len: 44
▼ Telnet
    Data:
    Data: \001\357\277\275\357\277\275-- \003\b\023krebsonsecurity.com\a\00280\030\003100

0000  08 00 27 65 4b ce 08 00  27 4d 0a bb 08 00 45 00   ..'eK... 'M....E.
0010  00 60 b6 38 40 00 40 06  6f d7 0a 10 00 64 0a 10   .`.8@.@. o....d..
0020  00 05 00 17 d5 7a d9 27  8b 0f 79 1d 50 47 80 18   .....z.' ..y.PG..
0030  01 c5 14 db 00 00 01 01  08 0a 00 0f f5 8f 00 02   ........ ........
0040  93 00 00 2c 00 00 00 64  0a 01 82 d3 2d 2d 20 03   ...,...d ....-- .
0050  08 13 6b 72 65 62 73 6f  6e 73 65 63 75 72 69 74   ..krebso nsecurit
0060  79 2e 63 6f 6d 07 02 38  30 18 03 31 30 30         y.com..8 0..100
```

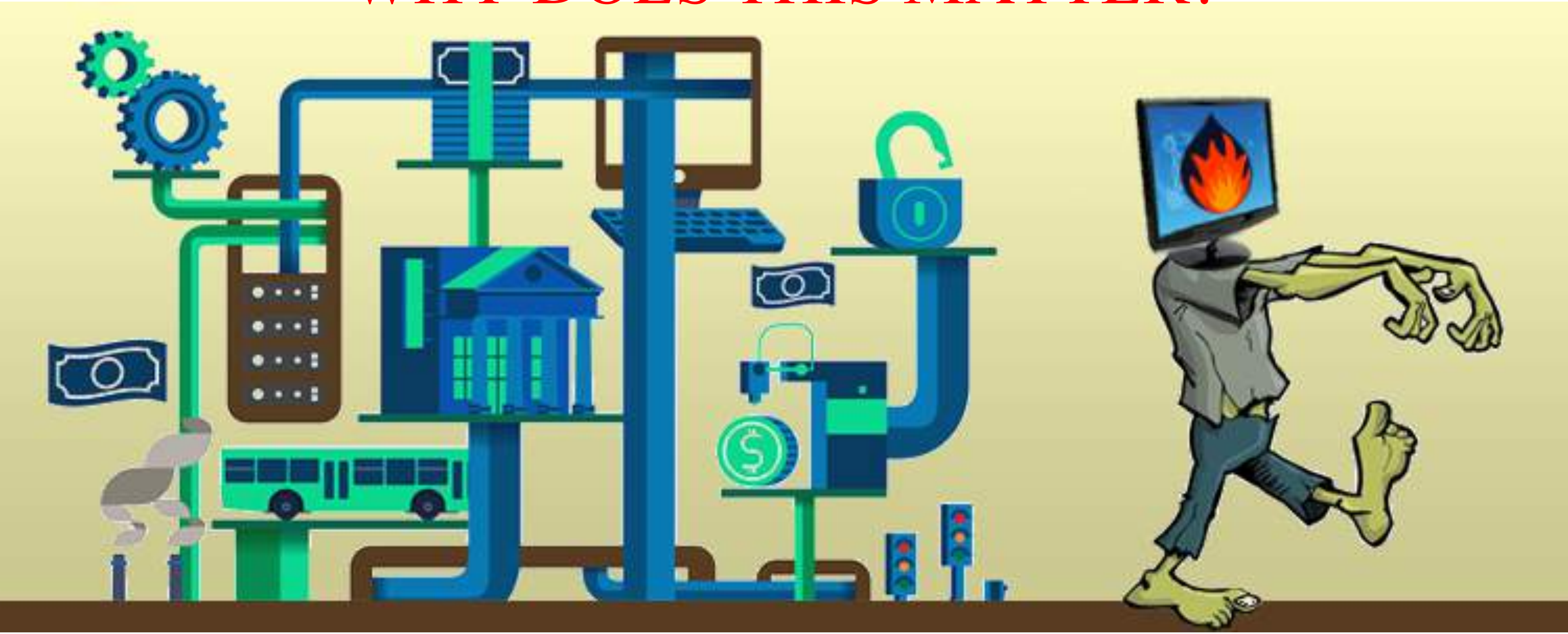
```
0000    00 2c 00 00 00 64 0a 01 82 d3 2d 2d 20 03 08 13  .,...d....-- ...
0010    6b 72 65 62 73 6f 6e 73 65 63 75 72 69 74 79 2e  krebsonsecurity.
0020    63 6f 6d 07 02 38 30 18 03 31 30 30              com..80..100
```

Targets and attack type
Total Length
Duration
Attack Type
Number of targets
Target + NM

Options Section
Num Options
Type
0x08 = hostname
0x07 = port
0x18 = number of connections
Option Value Length
Option Value

Motivation

WHY DOES THIS MATTER?



OWN YOUR NETWORK

Reasonable security resides somewhere along this spectrum!

Brilliance in the Basics

- Cause we don’t have $$$ like the big Companies
- WIRESHARK should be the first thing you go to!!!!
- You are the C-suite of your house, ask the hard questions ➔ are we Secure? Resilient? Recoverable?
- Prevent, Detect, Respond
- Need to get repetitions with this technology/skill set

Within budget? Oops, don’t let the “real” bosses of the households know that we are buying some toys to play with!

Objective

- Conduct capture and analysis to baseline your network
  - Proactive vs. reactive capture
  - Passive vs. active recon
  - Traffic or more fine grained ➔ OS/physical devices
  - Key items - top talkers, BWOT, protocol distributions, applications, ground truth of network diagram, start up of OS/system
- Determine normal behavior, non-malicious traffic
- So you can ID unusual protocols and unrecognized port numbers
  - BOTs phoning home or worse DOSing Krebs
  - RATs
  - Covert channels

Packing List

- HW
  - Hubs, TAPs, switch capable of mirroring, wireless capture device
  - Laptop with a good NIC and processing power
  - Good cables
- SW
  - ***WIRESHARK!!!!!!!!***
  - Dumpcap/tcpdump, nmap, Packet Analyzer
  - Splunk, Bro, Surricata, Ntop

Controls

- pfSense
- DD-WRT/OpenWRT
- VLANs
- Managed or smart switches
- Firewall ACLs or whitelist
  - ➢UPnP == no no
  - ➢IOCs blocked, until further notice

Put ”bad” devices into time-out and make sure they can’t talk to any other devices.

Reassess

- IF Patch OR upgrade THEN re-baseline
- Security is a moving tgt, once you reach the hilltop, assess from your new vantage point and determine the next objective
- Hardening your defensive position is continuous

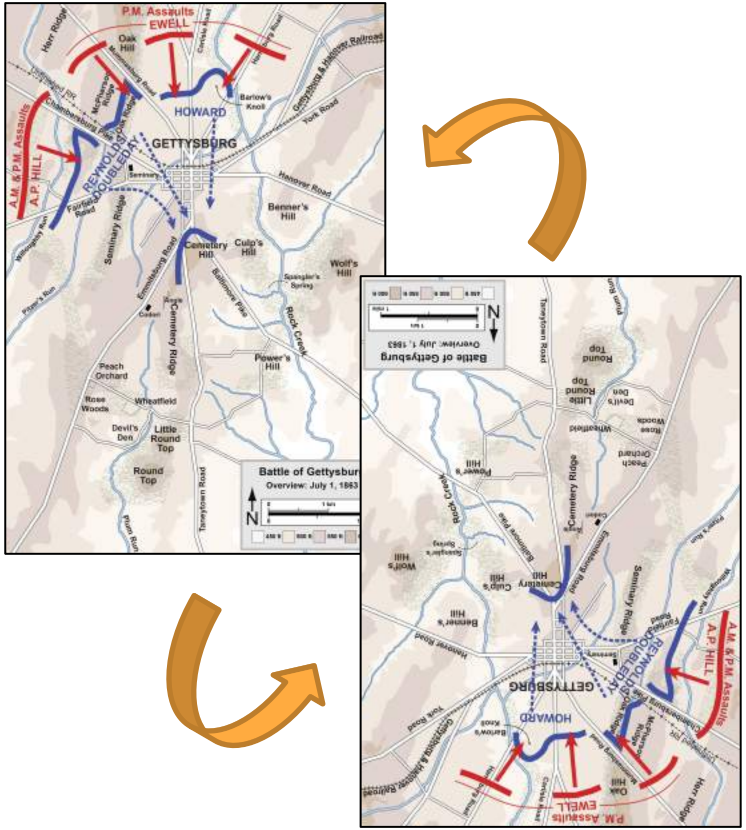
PWN YOUR NETWORK

Switching Roles

- The value of turning the map around on ourselves

- 5 Phases of Ethical Hacking
  1. Reconnaissance
  2. Scanning
  3. Gaining Access
  4. ~~Maintaining Access~~
  5. ~~Covering Tracks~~

We will be focusing on these three during the demo portion.

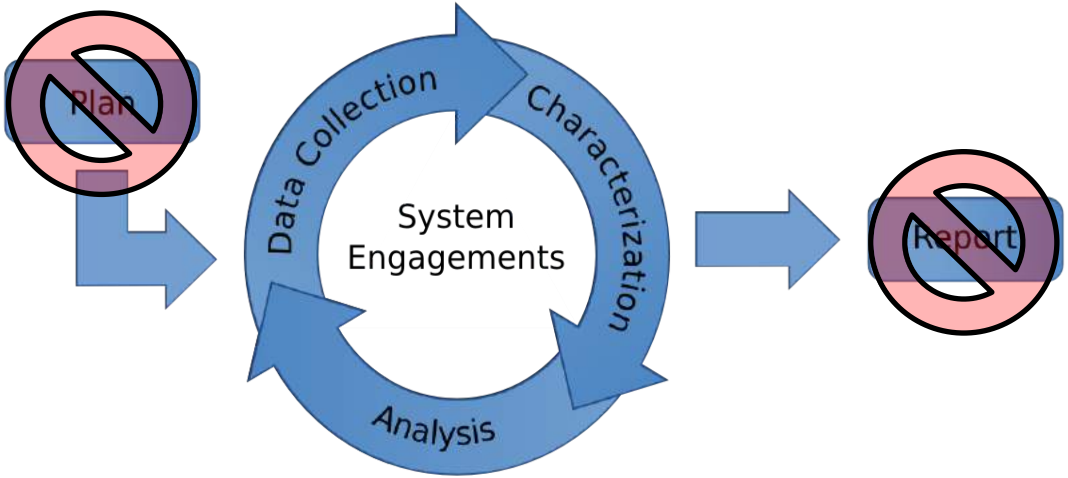


Reconnaissance

- Passive is already done
  - What did we see? What jumped out?
- Active recon
  - Nmap
  - Nessus
- Take that flagged/interesting traffic and see what hits are on the vulnerability databases
  - NIST NVD
  - CVE
  - Offensive Security Exploit DB
- Make your high value target hit list

Vulnerability Research/ Exploitation

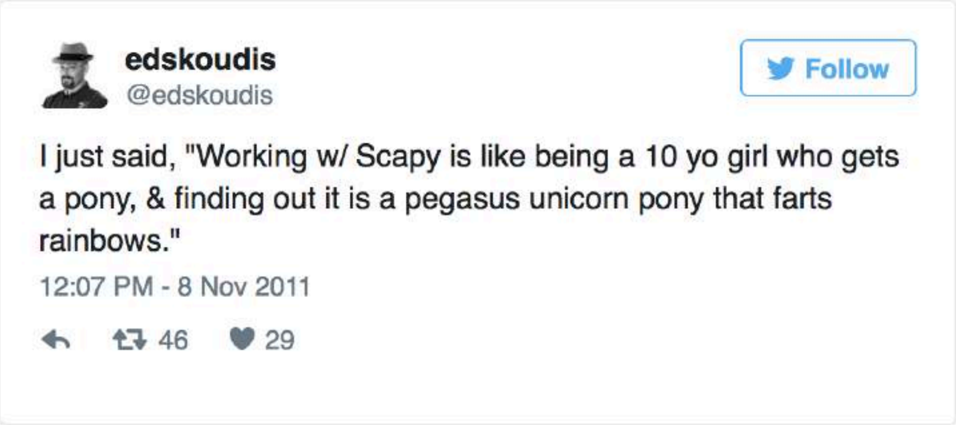
- This is the engagement – hypothesize, test/probe, analyze results, refine
- Sandia IDART Methodology



Seriously…this is a home hacking project! No formal plan, no reports. Just don't brick the network because it's Netflix night.

Scapy

- Great tool for “artisan” crafting of packets, against a specific target
  - ➢Forgery
  - ➢Sniffing
  - ➢Dissecting
  - ➢Sending
  - ➢Real time interaction with target
  - ➢Flexible building of protocols, potential abuse of RFCs
- Adult LEGOs



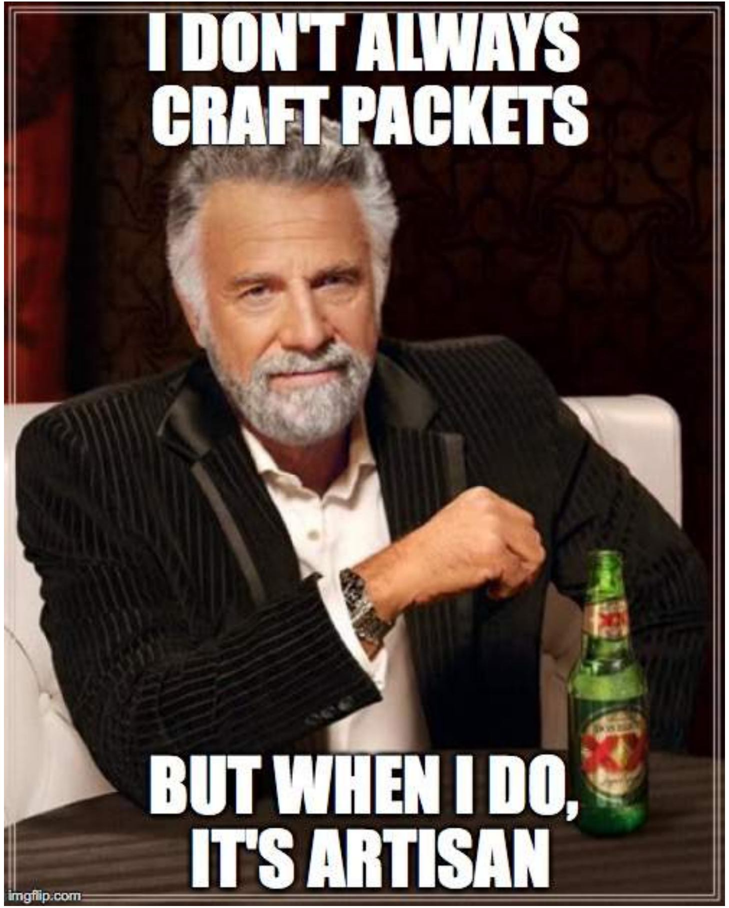
edskoudis
@edskoudis

I just said, "Working w/ Scapy is like being a 10 yo girl who gets a pony, & finding out it is a pegasus unicorn pony that farts rainbows."

12:07 PM - 8 Nov 2011

46 29

Let the Packet Crafting Begin

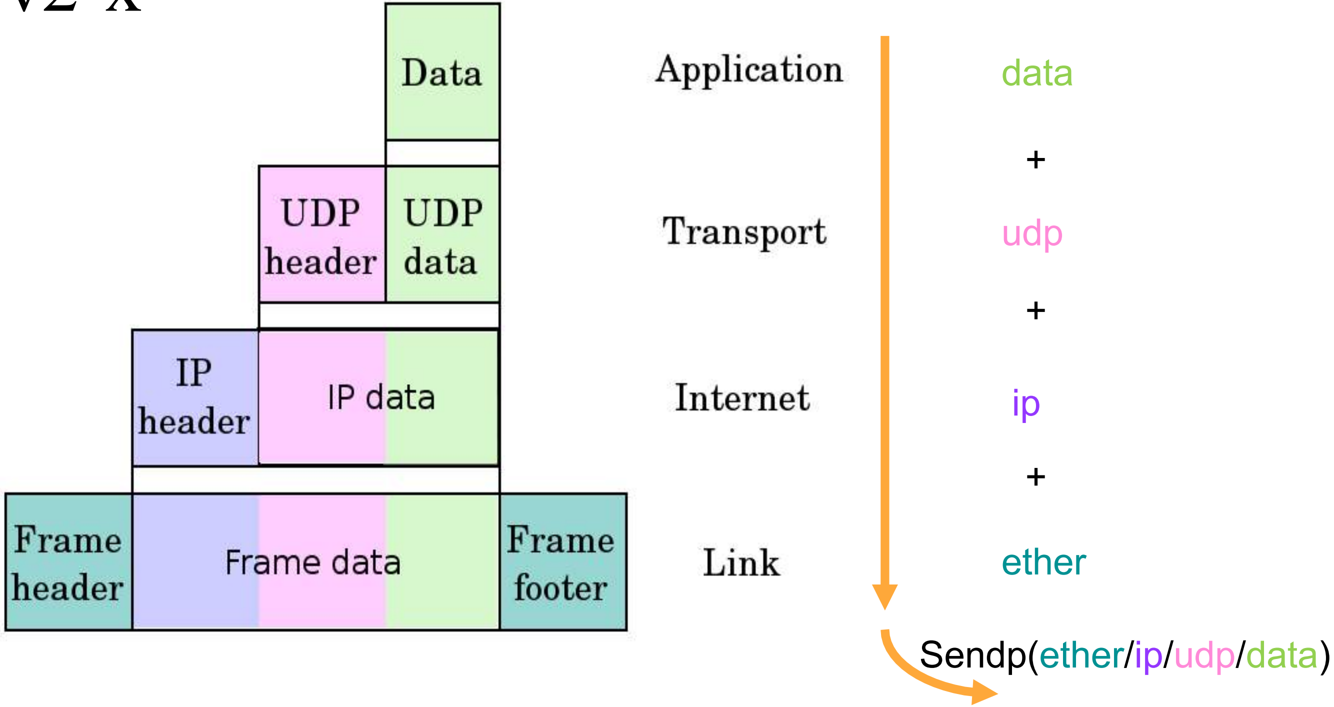


Scapy Crash Course

- http://scapy.readthedocs.io/en/latest/installation.html#installing-scapy-v2-x
- Mental model

-Not meant to analyze large captures, since it is a memory hog

-Not designed for high throughput, Python is not a “lean” program



Application

Transport

Internet

Link

data

+

udp

+

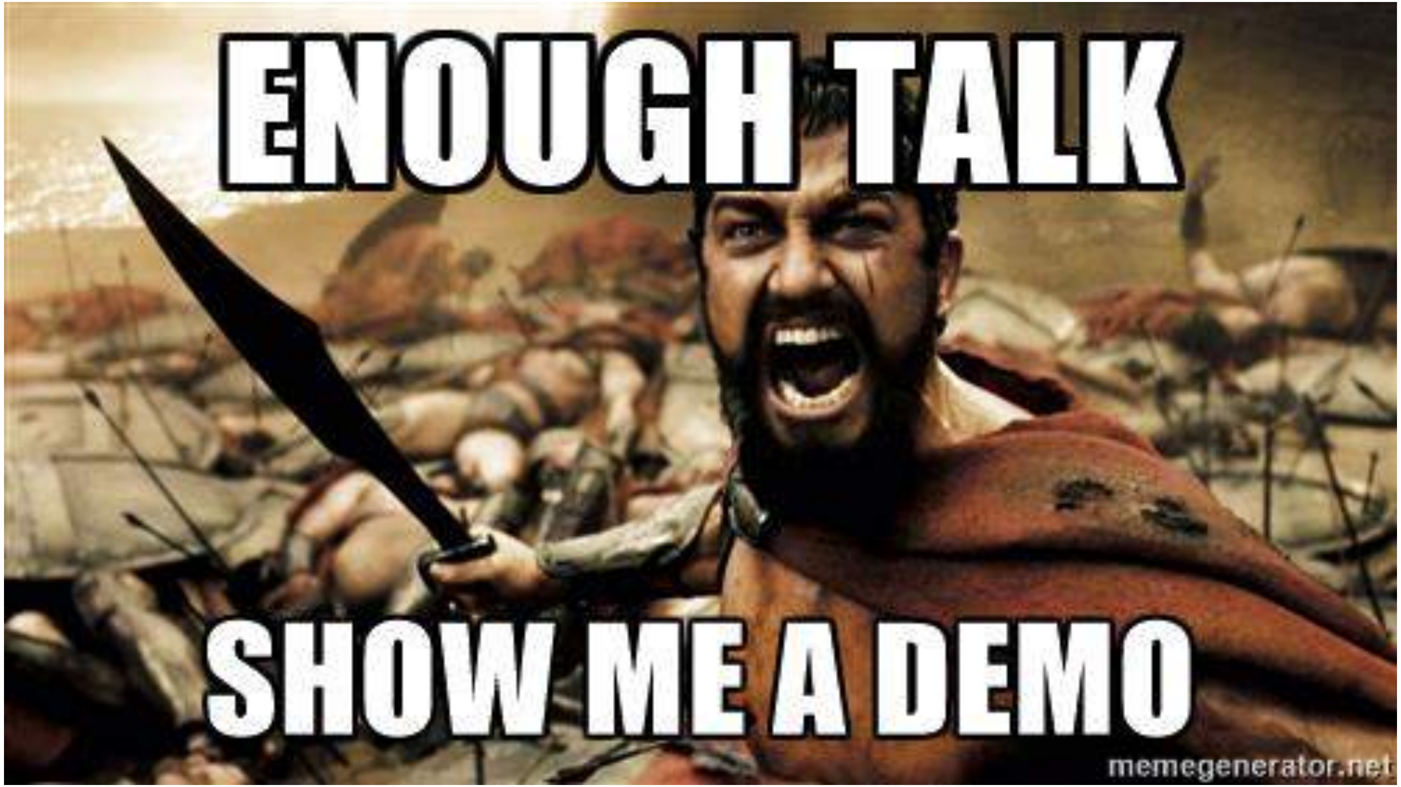
ip

+

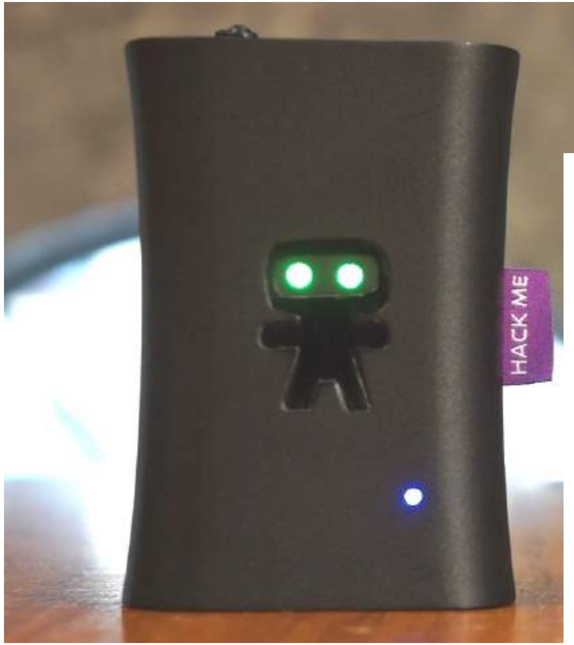
ether

Sendp(ether/ip/udp/data)

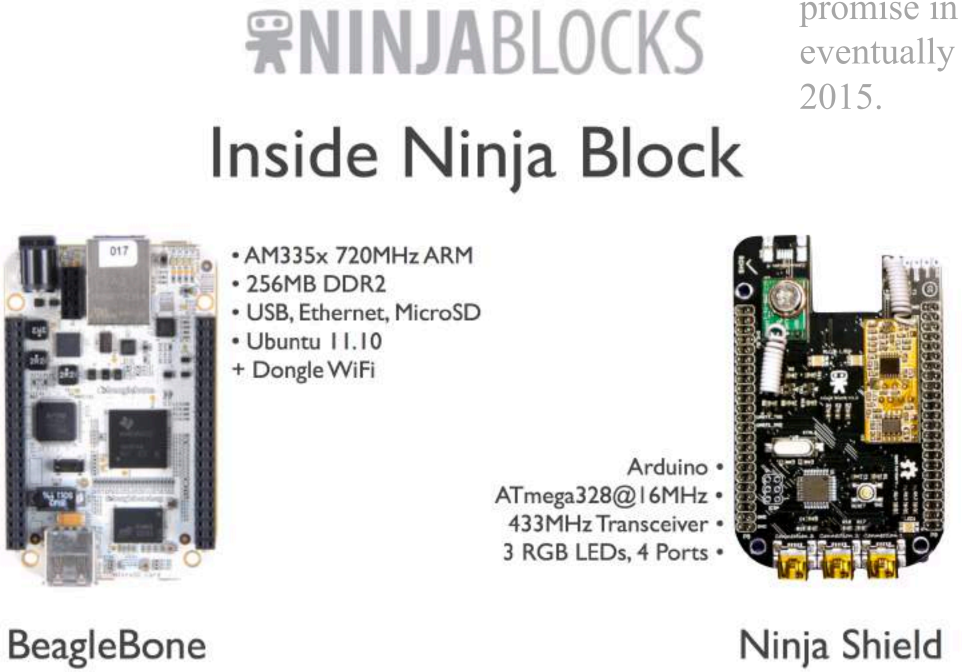
LAB TIME



Scenario



Meet Nina the NinjaBlock. This was a crowd funded IoT project that showed a lot of promise in 2012, but eventually fizzled out in 2015.



NINJABLOCKS

Inside Ninja Block

- AM335x 720MHz ARM
- 256MB DDR2
- USB, Ethernet, MicroSD
- Ubuntu 11.10

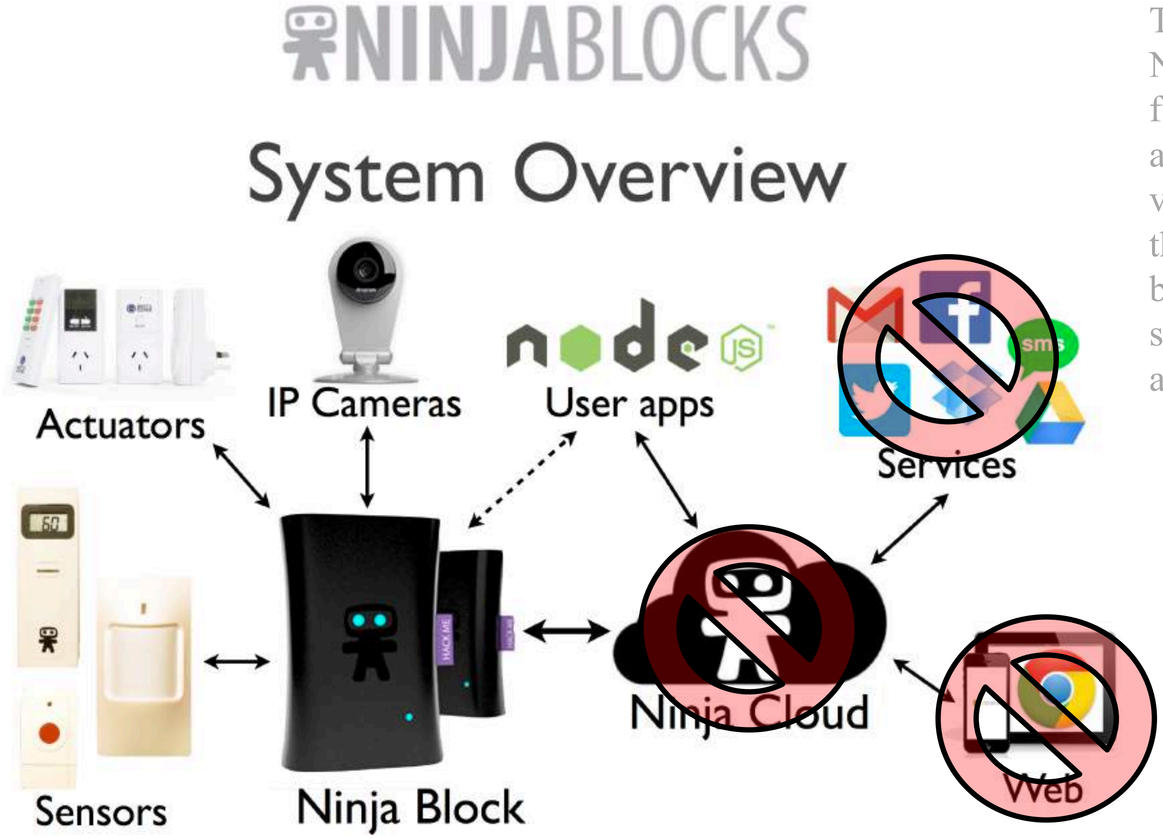
+ Dongle WiFi

BeagleBone

- Arduino
- ATmega328@16MHz
- 433MHz Transceiver
- 3 RGB LEDs, 4 Ports

Ninja Shield

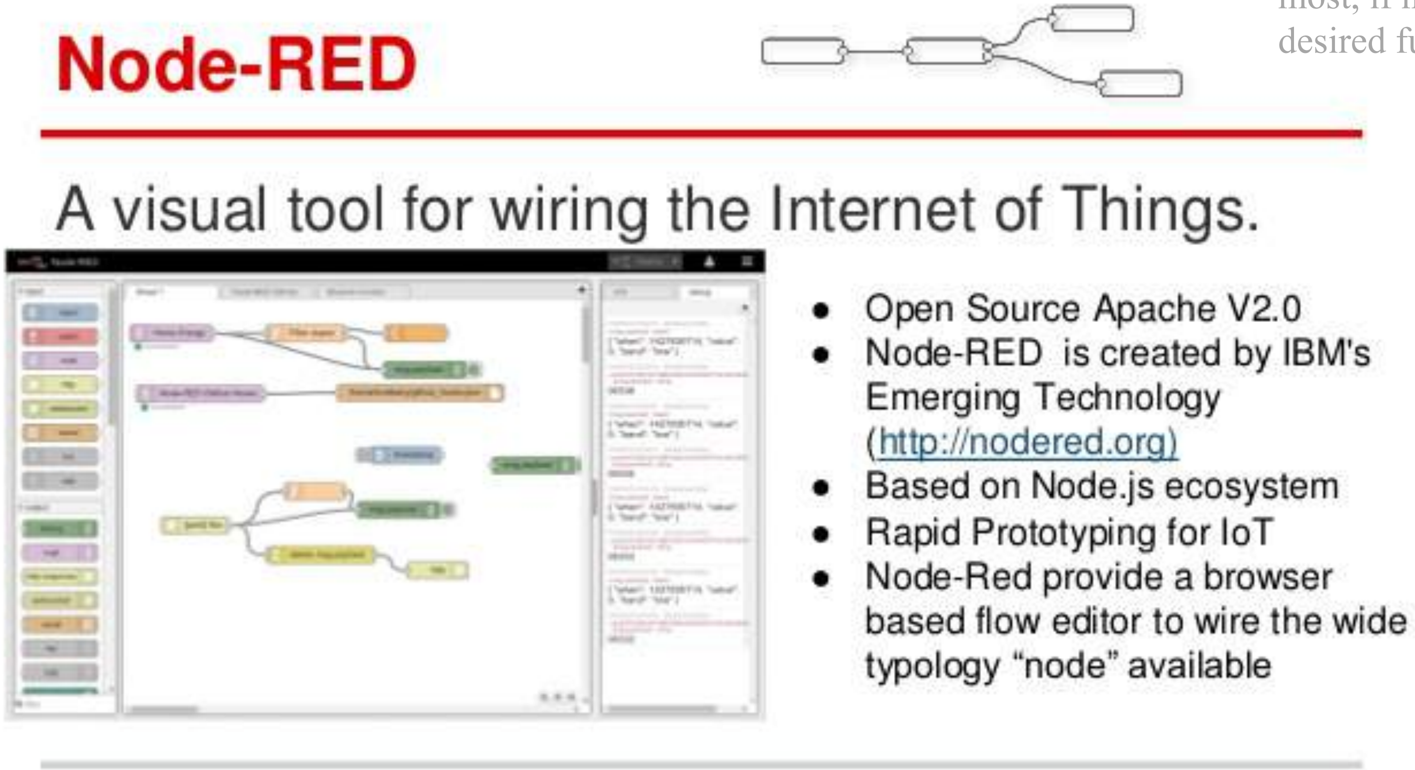
Scenario Cont'd



These systems gave the NinjaBlock the functionality to automate and control various things. Once they went down, backers had to scramble to find an alternative.

Scenario Cont’d

Node-Red provides most, if not all, of the desired functionality.



Node-RED

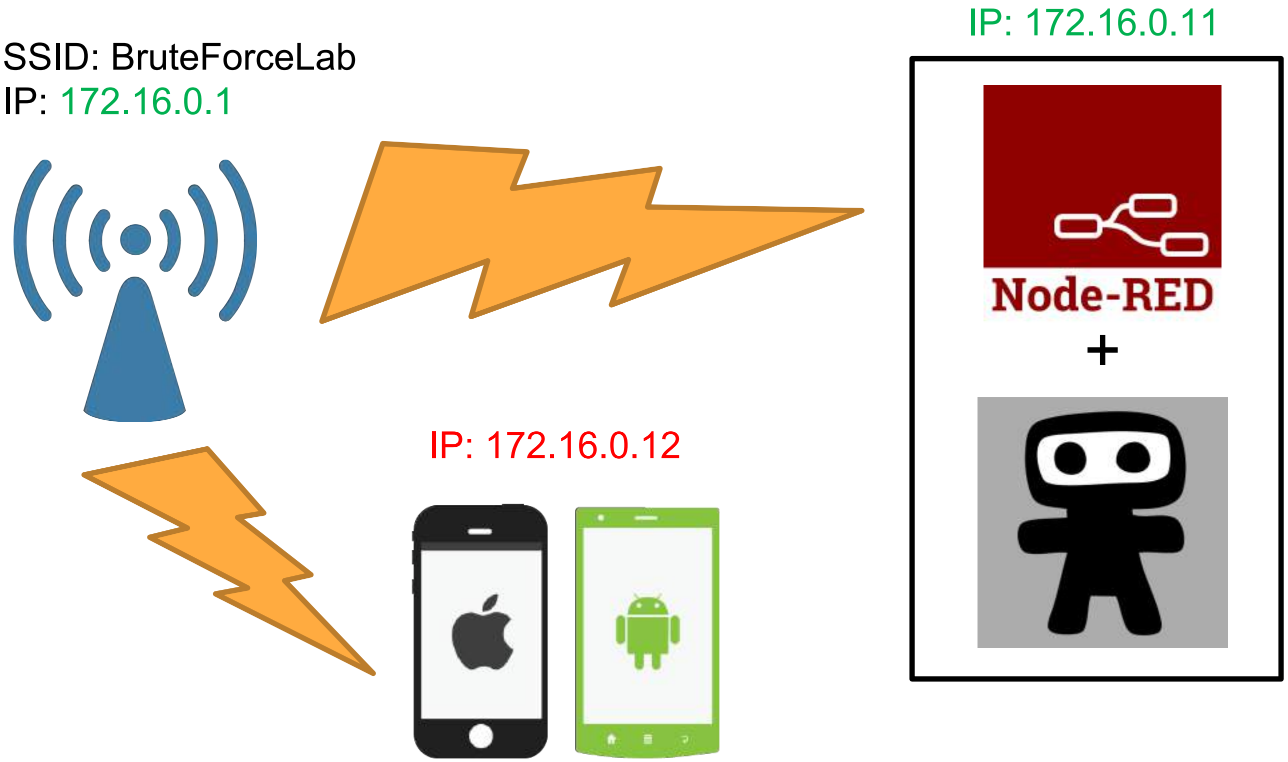
A visual tool for wiring the Internet of Things.

- Open Source Apache V2.0
- Node-RED is created by IBM's Emerging Technology (http://nodered.org)
- Based on Node.js ecosystem
- Rapid Prototyping for IoT
- Node-Red provide a browser based flow editor to wire the wide typology “node” available

Rules of Engagement (ROE)

- BruteForceLab AP – only AP you should be associating with to conduct sniffing/injecting
- NinjaBlock IP – only IP that you should be targeting
- Pls respect these rules and do not act maliciously towards your neighbors & peers

Network Diagram



Resources

- OSint – GOOGLE, beaglebone.com, ninjablock forums
- Scapy {https://blogs.sans.org/pen-testing/files/2016/04/ScapyCheatSheet_v0.2.pdf} ||
  {http://packetlife.net/media/library/36/scapy.pdf}
- Nmap {https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.0.pdf} ||
  {$ man nmap}

How Did It Go?

YOU WENT FULL ARTISAN
NEVER GO FULL ARTISAN
ARMY
memegenerator.net

¿ QUESTIONS ?

✉ brad@bruteforce.io

in linkedin.com/in/bradpalm/