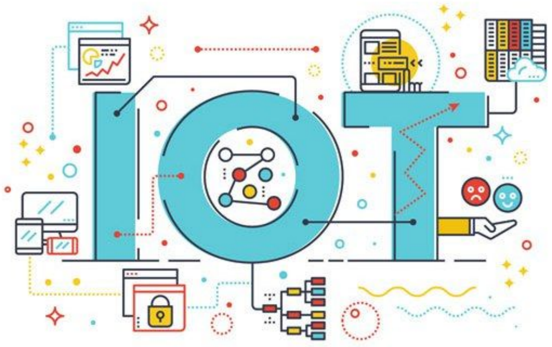


Hacking IoT Devices Methodology

LufSec

Disclaimer

The views expressed in this presentation are those of the author and do not reflect the official policy or position of Infineon Technologies

LufSec

Who Am I

- ❑ Head InfoSec Infineon Technologies Americas
- ❑ Founder LufSec
- ❑ Author (LinkedIn Learning)
- ❑ CISSP, CRISC, PCIP, CISM, CEH
- ❑ Husband, father hacker, love to teach & coach
- ❑ DEFCON Red Team Village Volunteer
- ❑ Member CSA IoT Security Group

CISSP® Certified Information Systems Security Professional

CRISC™ Certified in Risk and Information Systems Control™

CISM® Certified Information Security Manager® An ISACA® Certification

PCI Security Standards Council® PCI PROFESSIONAL (PCIP)™ PROGRAM

CEH™ Certified Ethical Hacker

Contact Information

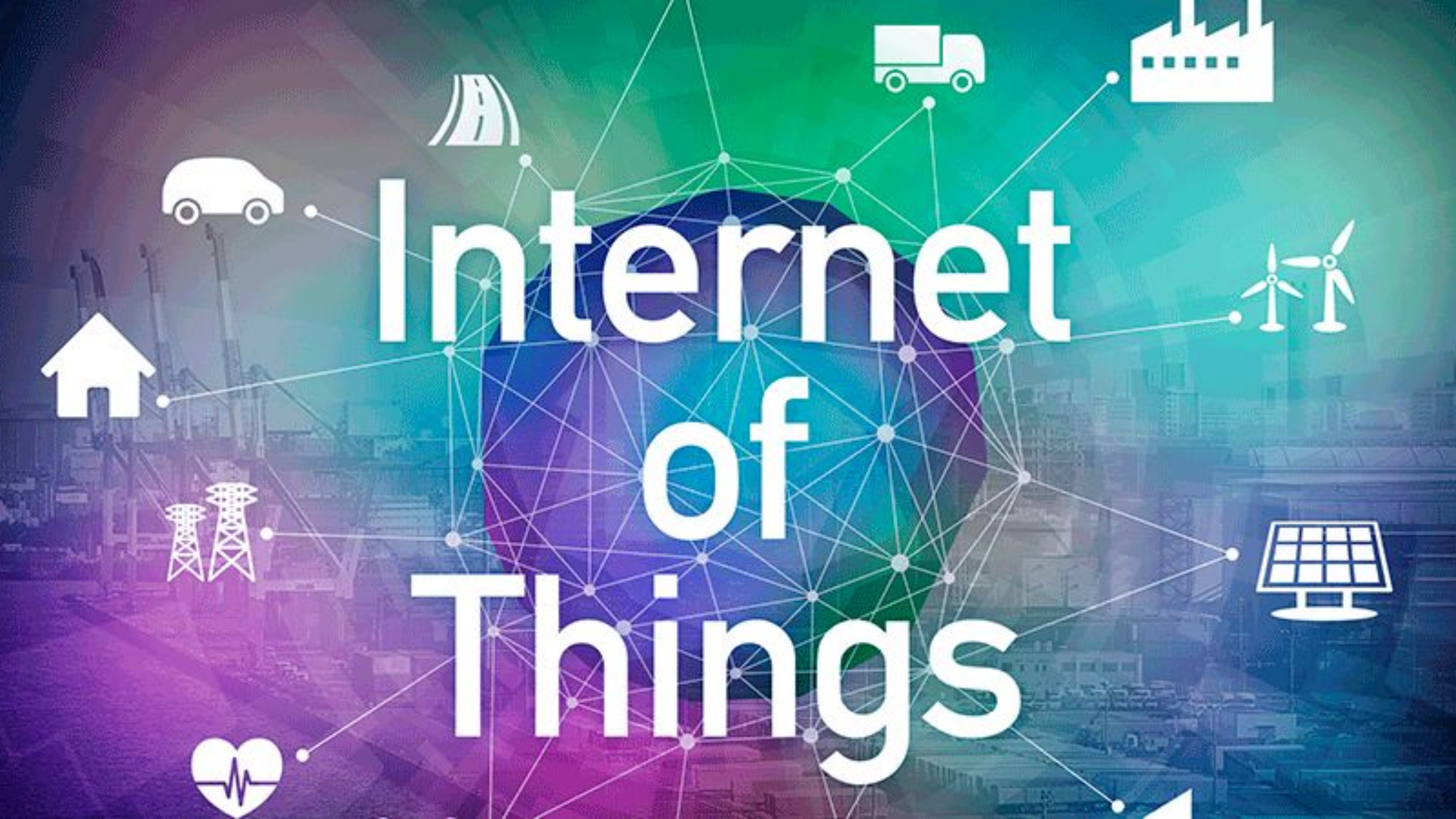
@lucianoferrari

linkedin.com/in/lucianoferrari

www.lufsec.com

lferrari@lufsec.com

github.com/lucianoferrari


Internet
of
Things

Wearables
Aerospace and Defense
Mobile Devices
Industrial
Wireless Infrastructure
Computing
Media
Machine-to-Machine
Smart Meters
Consumer Electronics
Medical
Automotive
Smart Energy
72
Connected Home
Networking

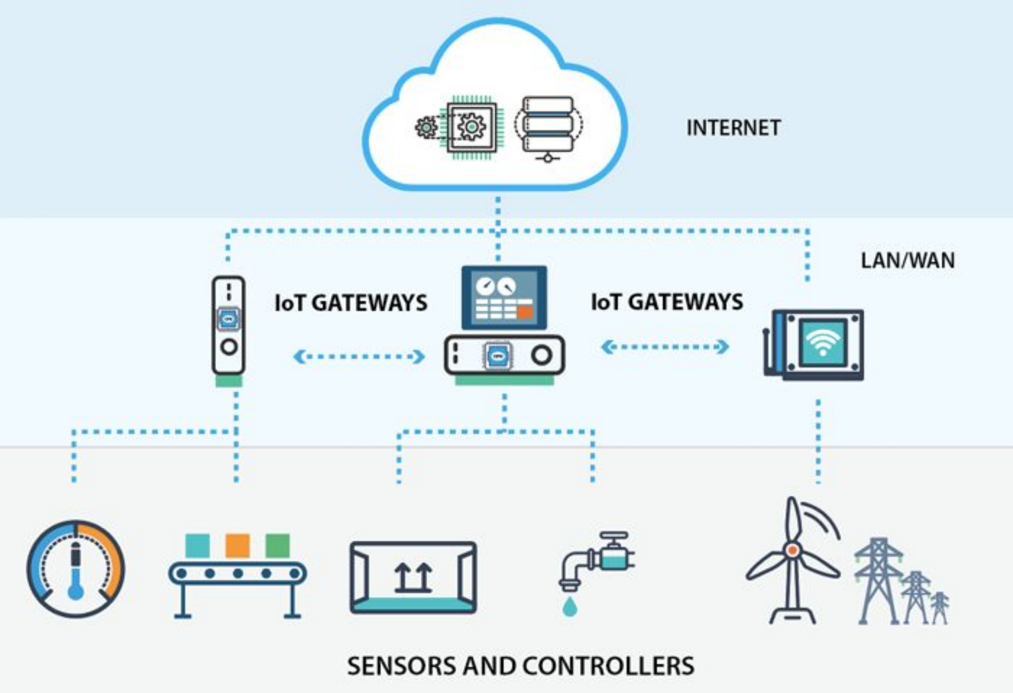
Why IoT Penetration Testing

- Understand Risks of IoT Devices to Organization
- Participate on Bug Bounties Program
- Product Security
- Challenge Yourself
- Get the Momentum

LufSec

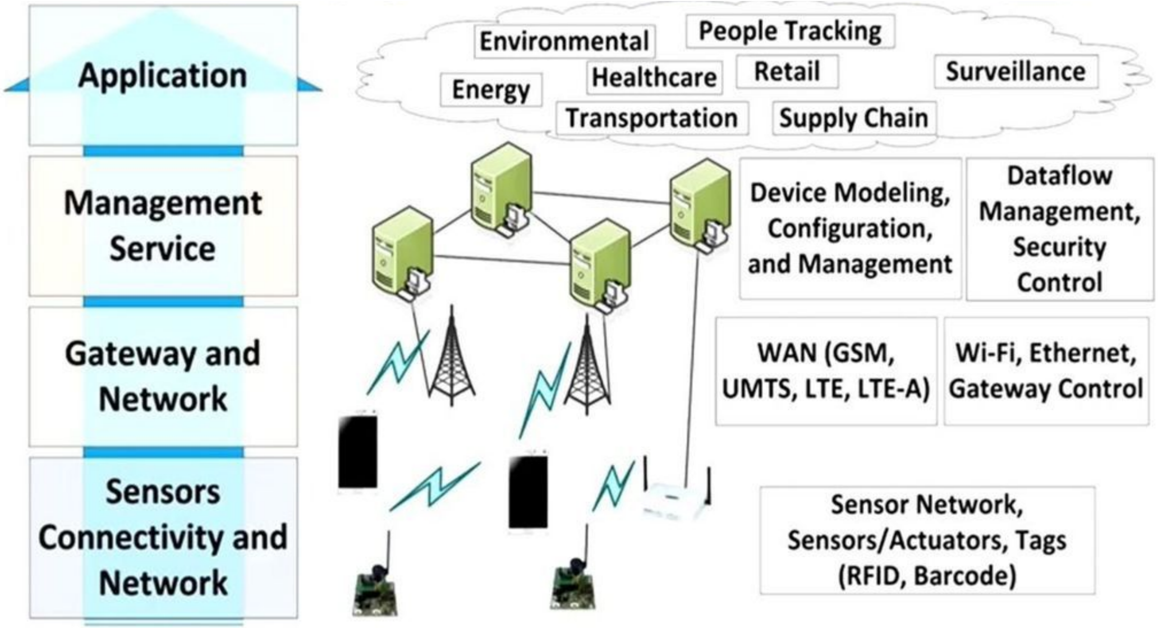
IoT Internet Connection

- Wired
- Wireless
- Gateway



LufSec

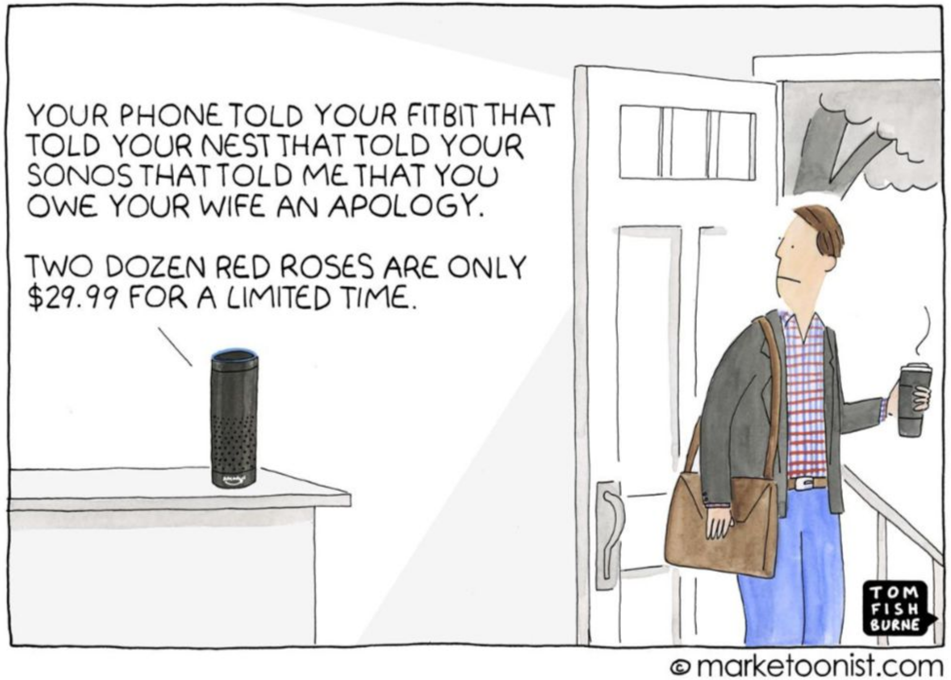
IoT Architecture Layers


Application
Management Service
Gateway and Network
Sensors Connectivity and Network
Environmental
People Tracking
Energy
Healthcare
Retail
Surveillance
Transportation
Supply Chain
Device Modeling, Configuration, and Management
Dataflow Management, Security Control
WAN (GSM, UMTS, LTE, LTE-A)
Wi-Fi, Ethernet, Gateway Control
Sensor Network, Sensors/Actuators, Tags (RFID, Barcode)

IoT Technologies and Protocols

Wireless Communication			Wired Communication	Operating System
Short Range	Medium Range	Long Range		
Bluetooth Low Energy (BLE)	HaLow	Low-Power Wide Area Network (LPWAN)	Ethernet	ARM Embedded OS
Light Fidelity (Li-Fi)	LTE Advanced	Very Small Aperture Terminal (VSAT)	Multimedia over Coax Alliance (MoCa)	Ubuntu Core
Near Field Communic. (NFC)		Cellular	Power Line Communication (PLC)	RIOT OS
Radio-Frequency Ident. (RFID)				RealSense OS X
Wi-Fi				Integrity RTOS

IoT Security Challenges


YOUR PHONE TOLD YOUR FITBIT THAT TOLD YOUR NEST THAT TOLD YOUR SONOS THAT TOLD ME THAT YOU OWE YOUR WIFE AN APOLOGY.
TWO DOZEN RED ROSES ARE ONLY $29.99 FOR A LIMITED TIME.
TOM FISH BURNE
© marketoonist.com

IoT Security Challenges

- Understand how the device works (operate, communicate)
- Vulnerable interfaces (web interfaces, APIs)
- Inefficient physical security protections (install backdoors)
- Insufficient vendor support
- Lack of or inefficient firmware/OS updates
- Interoperability Issues (vendor-centric solutions)

OWASP IoT Top 10

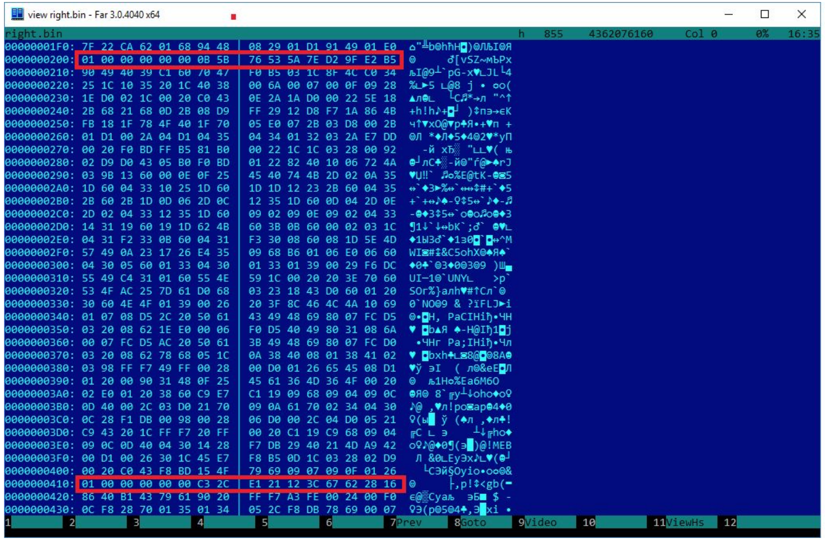
1. Weak Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

OWASP

Internet of Things Top 10

IoT Attack Surface

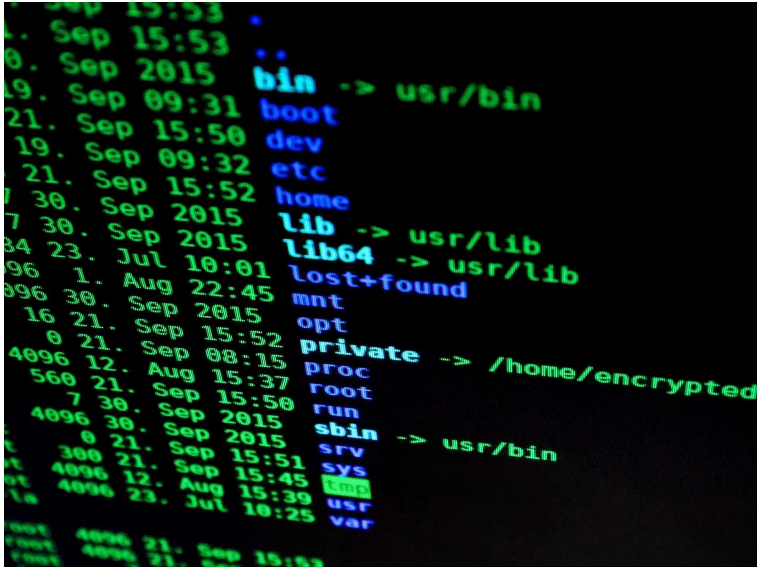
- Device memory containing credentials
- Access Control
- Firmware Extraction
- Privilege Escalation
- Resetting to an insecure state
- Web Attacks
- Firmware Attacks



```
right.bin                                                          h    855    4362076160    Col 0    0%    16:35
00000001F0: 7F 22 CA 62 01 68 94 48 | 08 29 01 D1 91 49 01 E0  ⌂"╩b☺hħH◘)☺ЛЉI☺Я
0000000200: 01 00 00 00 00 00 0B 5B | 76 53 5A 7E D2 9F E2 B5  ☺      ♂[vSZ~мЪPх
0000000210: 90 49 40 39 C1 60 70 47 | F0 B5 03 1C 8F 4C C0 34  ЉI@9┴`pG-х♥∟JL└4
0000000220: 25 1C 10 35 20 1C 40 38 | 00 6A 00 07 00 0F 09 28  %∟►5 ∟@8 j • ☼○(
0000000230: 1E D0 02 1C 00 20 C0 43 | 0E 2A 1A D0 00 22 5E 18  ▲л☻∟ └C♫*→л "^↑
0000000240: 2B 68 21 68 0D 2B 08 D9 | FF 29 12 D8 F7 1A 86 4B  +h!h♪+◘┘ )↕пэ→єK
0000000250: FB 18 1F 78 4F 40 1F 70 | 05 E0 07 2B 03 D8 00 2B  ч↑▼xO@▼p♣Я•+♥п +
0000000260: 01 D1 00 2A 04 D1 04 35 | 04 34 01 32 03 2A E7 DD  ☺Л *♦Л♦5♦4☺2♥*уП
0000000270: 00 20 F0 BD FF B5 81 B0 | 00 22 1C 1C 03 28 00 92   -й хЂ░ "∟∟♥( њ
0000000280: 02 D9 D0 43 05 B0 F0 BD | 01 22 82 40 10 06 72 4A  ☻┘лC♣░-й☺"ѓ@►♠rJ
0000000290: 03 9B 13 60 00 0E 0F 25 | 45 40 74 4B 2D 02 0A 35  ♥џ‼` ♫☼%E@tK-☻◙5
00000002A0: 1D 60 04 33 10 25 1D 60 | 1D 1D 12 23 2B 60 04 35  ↔`♦3►%↔`↔↔↕#+`♦5
00000002B0: 2B 60 2B 1D 0D 06 2D 0C | 12 35 1D 60 0D 04 2D 0E  +`+↔♪♠-♀↕5↔`♪♦-♫
00000002C0: 2D 02 04 33 12 35 1D 60 | 09 02 09 0E 09 02 04 33  -☻♦3↕5↔`○☻○♫○☻♦3
00000002D0: 14 31 19 60 19 1D 62 4B | 60 3B 0B 60 00 02 03 1C  ¶1↓`↓↔bK`;♂` ☻♥∟
00000002E0: 04 31 F2 33 0B 60 04 31 | F3 30 08 60 08 1D 5E 4D  ♦1Ы3♂`♦1э0◘`◘↔^M
00000002F0: 57 49 0A 23 17 26 E4 35 | 09 68 B6 01 06 E0 06 60  WI◙#↨&C5ohX☺♠Я♠`
0000000300: 04 30 05 60 01 33 04 30 | 01 33 01 39 00 29 F6 DC  ♦0♣`☺3♦0☺3☺9 )Ш▄
0000000310: 55 49 C4 31 01 60 55 4E | 59 1C 00 20 20 3E 70 60  UI─1☺`UNY∟   >p`
0000000320: 53 4F AC 25 7D 61 D0 68 | 03 23 18 43 D0 60 01 20  SOг%}aлh♥#↑Cл`☺
0000000330: 30 60 4E 4F 01 39 00 26 | 20 3F 8C 46 4C 4A 10 69  0`NO☺9 & ?ЊFLJ►i
0000000340: 01 07 08 D5 2C 20 50 61 | 43 49 48 69 80 07 FC D5  ☺•◘Н, PaCIHiЂ•ЧН
0000000350: 03 20 08 62 1E E0 00 06 | F0 D5 40 49 80 31 08 6A  ♥ ◘b▲Я ♠-Н@IЂ1◘j
0000000360: 00 07 FC D5 AC 20 50 61 | 3B 49 48 69 80 07 FC D0   •ЧНг Pa;IHiЂ•Чл
0000000370: 03 20 08 62 78 68 05 1C | 0A 38 40 08 01 38 41 02  ♥ ◘bxh♣∟◙8@◘☺8A☻
0000000380: 03 98 FF F7 49 FF 00 28 | 00 D0 01 26 65 45 08 D1  ♥ў эI  ( л☺&eE◘Л
0000000390: 01 20 00 90 31 48 0F 25 | 45 61 36 4D 36 4F 00 20  ☺  љ1H☼%Ea6M6O
00000003A0: 02 E0 01 20 38 60 C9 E7 | C1 19 09 68 09 04 09 0C  ☻Я☺ 8`╔у┴↓○h○♦○♀
00000003B0: 0D 40 00 2C 03 D0 21 70 | 09 0A 61 70 02 34 04 30  ♪@ ,♥л!p○◙ap☻4♦0
00000003C0: 0C 28 F1 DB 00 98 00 28 | 06 D0 00 2C 04 D0 05 21  ♀(ы█ ў (♠л ,♦л♣!
00000003D0: C9 43 20 1C FF F7 20 FF | 00 20 C1 19 C9 68 09 04  ╔C ∟ э     ┴↓╔h○♦
00000003E0: 09 0C 0D 40 04 30 14 28 | F7 DB 29 40 21 4D A9 42  ○♀♪@♦0¶(э█)@!MЕB
00000003F0: 00 D1 00 26 30 1C 45 E7 | F8 B5 0D 1C 03 28 02 D9   Л &0∟Eуэх♪∟♥(☻┘
0000000400: 00 20 C0 43 F8 BD 15 4F | 79 69 09 07 09 0F 01 26   └Cэй§Oyio•○☼☺&
0000000410: 01 00 00 00 00 00 C3 2C | E1 21 12 3C 67 62 28 16  ☺     ├,p!↕<gb(▬
0000000420: 86 40 B1 43 79 61 90 20 | FF F7 A3 FE 00 24 00 F0  є@▒Cyaљ эБ■ $ -
0000000430: 0C F8 28 70 01 35 01 34 | 05 2C F8 DB 78 69 00 07  ♀э(p☺5☺4♣,э█xi •
1        2        3        4        5        6        7Prev    8Goto    9Video   10       11ViewHs 12
```

IoT Attack Surface

- Network Services Attacks
- Unencrypted local data storage
- Confidentiality and Integrity Issues
- Cloud Computing Attack
- Malicious Updates
- Insecure APIs
- Mobile Application Threats



```
  Sep 15:53 .
1. Sep 15:53 ..
0. Sep 2015 bin -> usr/bin
19. Sep 09:31 boot
21. Sep 15:50 dev
19. Sep 09:32 etc
21. Sep 15:52 home
7 30. Sep 2015 lib -> usr/lib
7 30. Sep 2015 lib64 -> usr/lib
34 23. Jul 10:01 lost+found
96 1. Aug 22:45 mnt
096 30. Sep 2015 opt
16 21. Sep 15:52 private -> /home/encrypted
0 21. Sep 08:15 proc
4096 12. Aug 15:37 root
560 21. Sep 15:50 run
7 30. Sep 2015 sbin -> usr/bin
4096 30. Sep 2015 srv
0 21. Sep 15:51 sys
300 21. Sep 15:45 tmp
4096 12. Aug 15:39 usr
4096 23. Jul 10:25 var
```

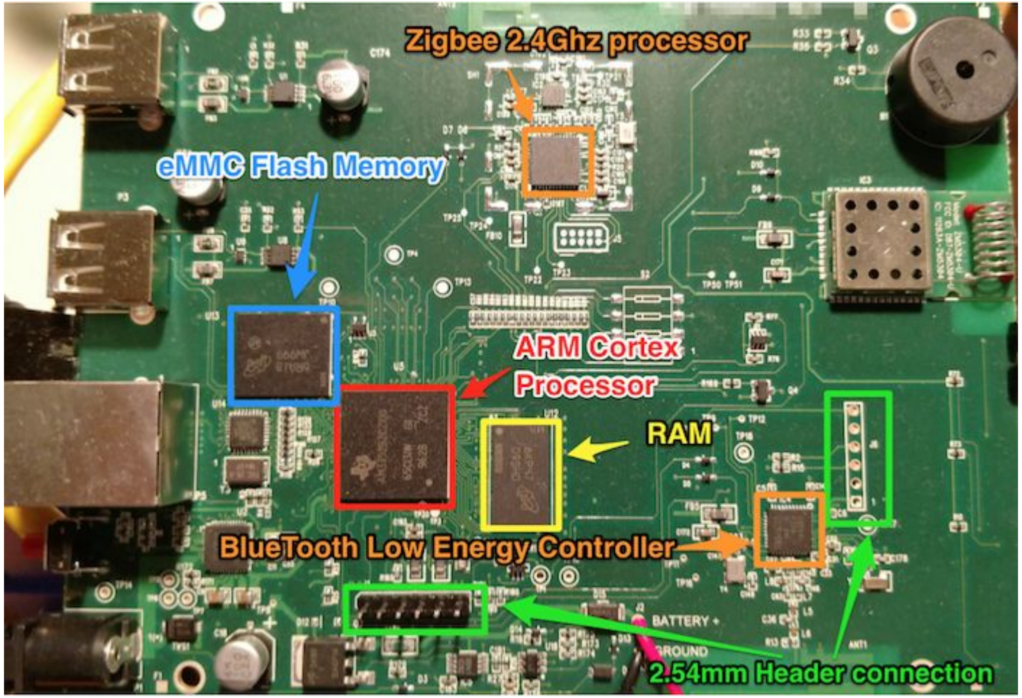
IoT Common Attacks

- DDoS
- Rolling Code
- BlueBorne
- Jamming
- Backdoor
- Eavesdropping

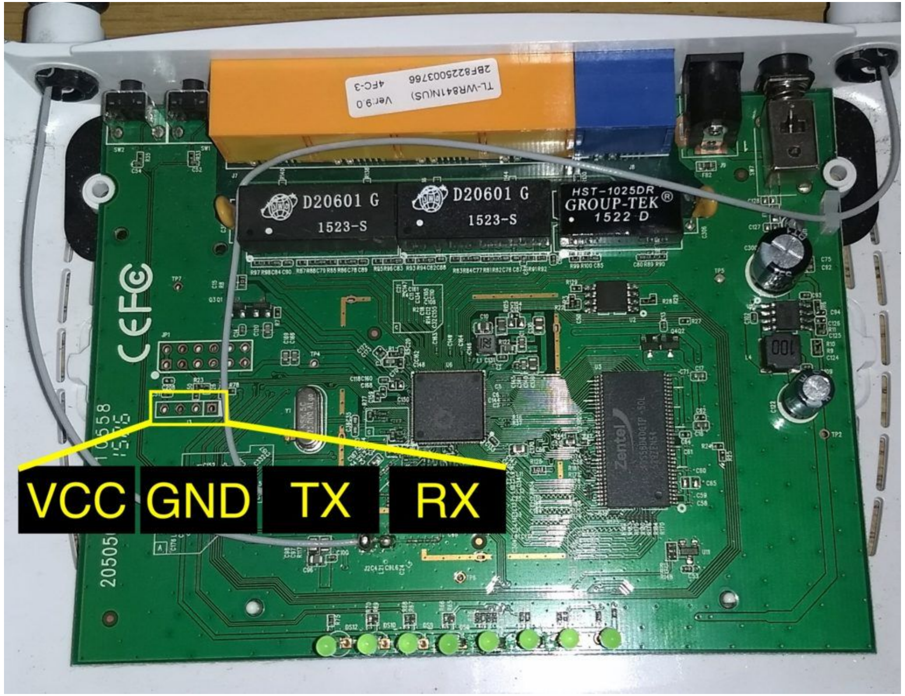
IoT Common Attacks

- Sybil
- Exploit Kits
- Man-in-the-Middle
- Forged Malicious Devices
- Side-channel
- Ransomware

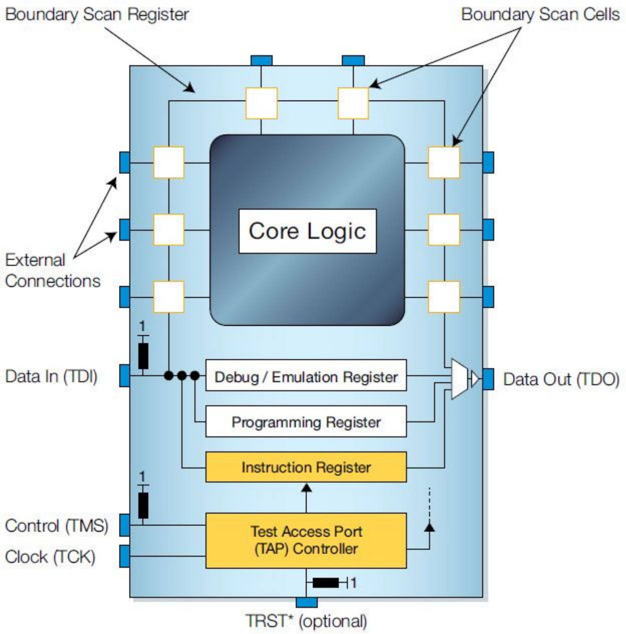
Hardware Components

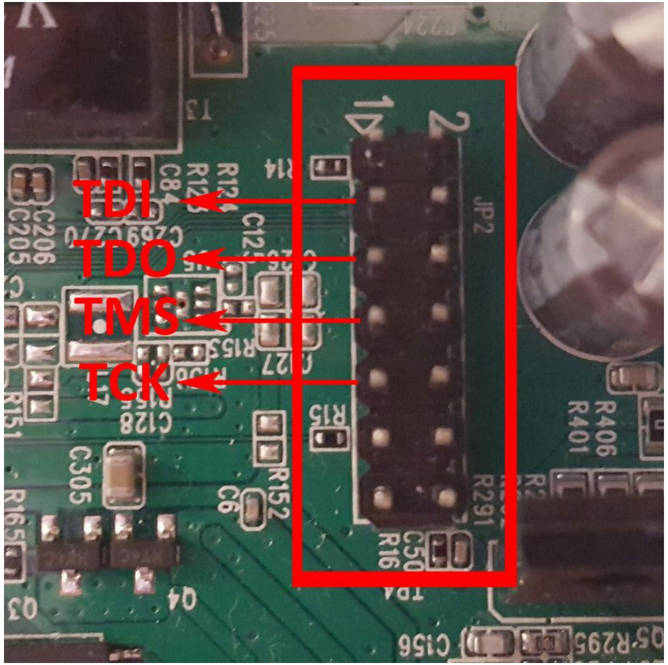


Hardware Components - UART

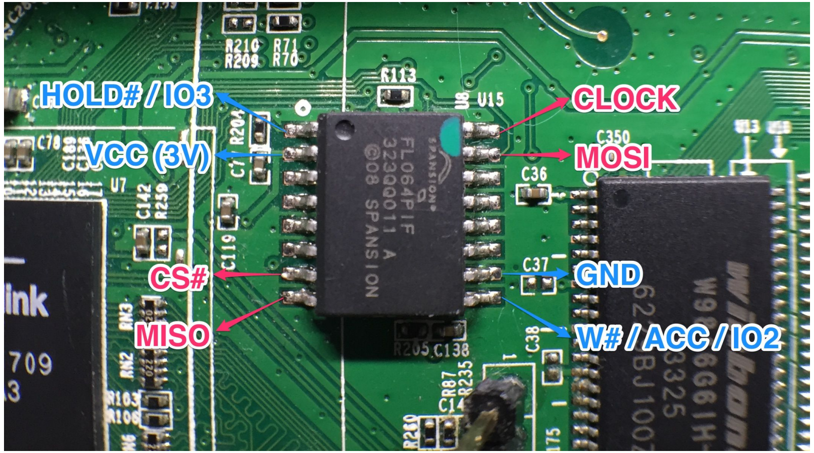


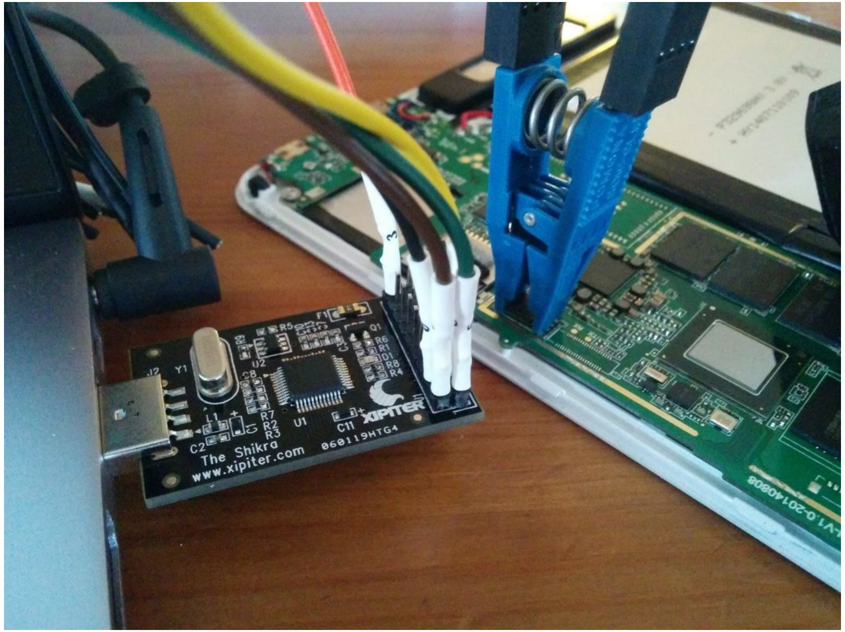
Hardware Components - JTAG



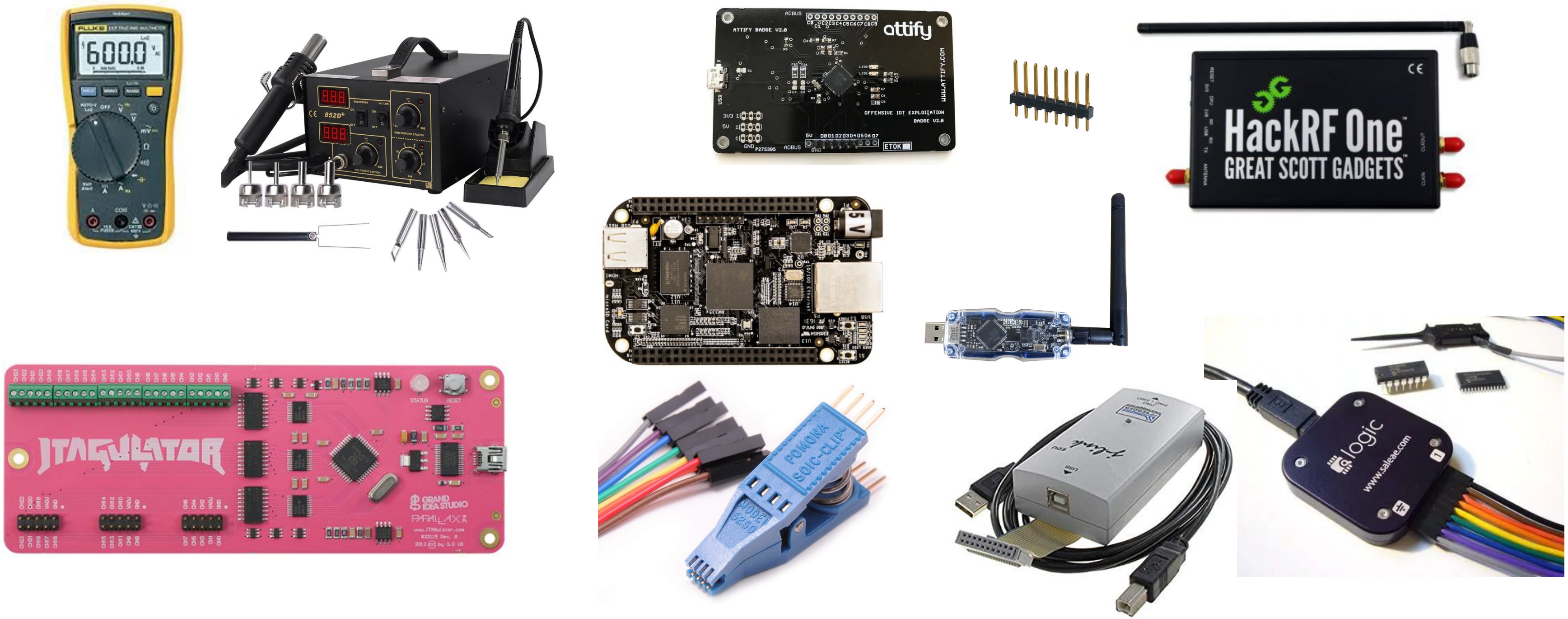


Hardware Components - SPI





Some Useful IoT Hacking Tools



IoT Hacking OS Platforms

- AttifyOS
- Kali Linux
- Ubuntu LTS
- Zephyr
- Skywave Linux
- Maintain Access

IoT Hacking Frameworks & other Tools

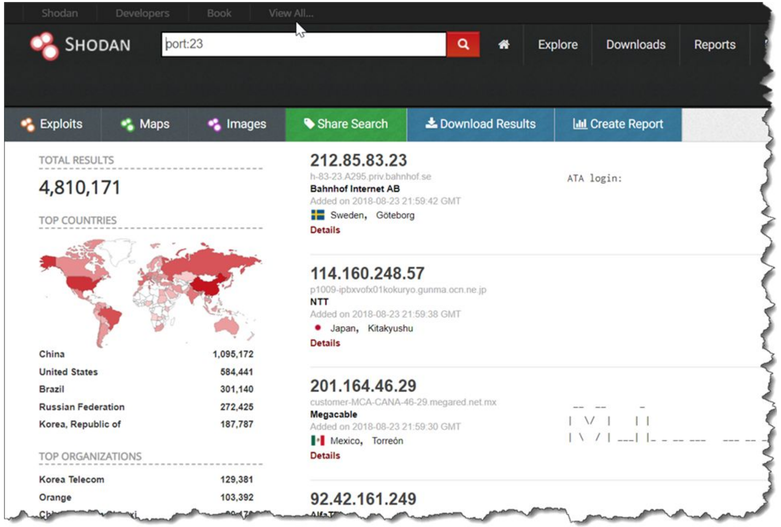
- IDA Pro
- Binary Ninja
- Radare2
- Ghidra
- GDB
- GnuRadio
- Nmap
- Routersploit
- Expliot Framework
- ...

IoT Hacking Methodology

- Information Gathering
- Vulnerability Scanning
- Launching Attack
- Gain Access
- Maintain Access

Information Gathering

- Understanding How the Device Operates
- FCC ID
- Datasheets & Manuals
- Shodan
- IP Addresses
- Running Protocol
- Vendor Site



TOTAL RESULTS

4,810,171

TOP COUNTRIES

China	1,095,172
United States	584,441
Brazil	301,140
Russian Federation	272,425
Korea, Republic of	187,787

TOP ORGANIZATIONS

Korea Telecom	129,381
Orange	103,392

212.85.83.23
h-83-23.A295.priv.bahnhof.se
Bahnhof Internet AB
Added on 2018-08-23 21:59:42 GMT
Sweden, Göteborg
Details

```
ATA login:
```

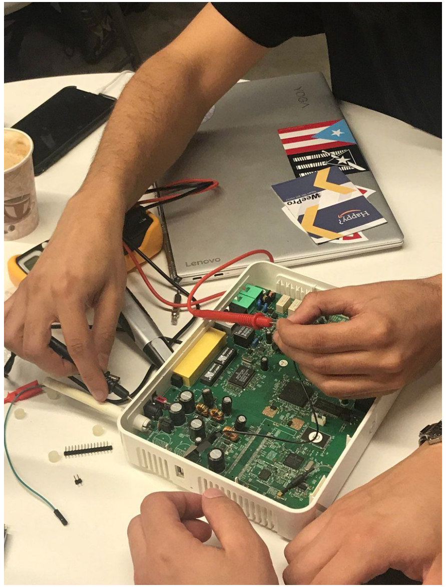
114.160.248.57
p1009-ipbxvofx01kokuryo.gunma.ocn.ne.jp
NTT
Added on 2018-08-23 21:59:38 GMT
Japan, Kitakyushu
Details

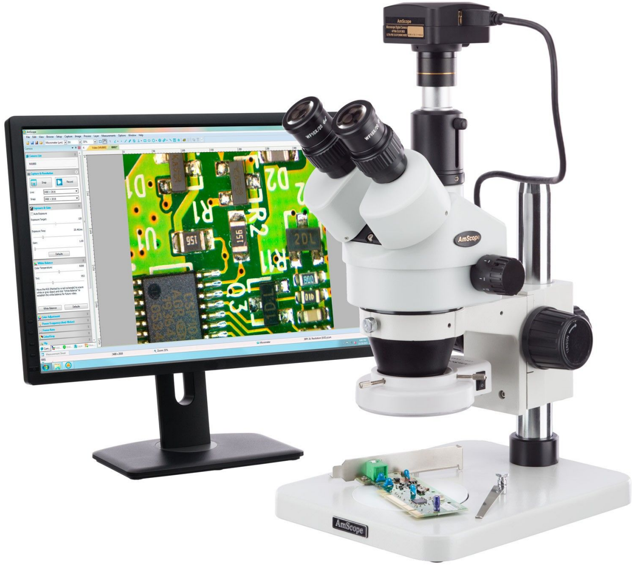
201.164.46.29
customer-MCA-CANA-46-29.megared.net.mx
Megacable
Added on 2018-08-23 21:59:30 GMT
Mexico, Torreón
Details

92.42.161.249

Information Gathering

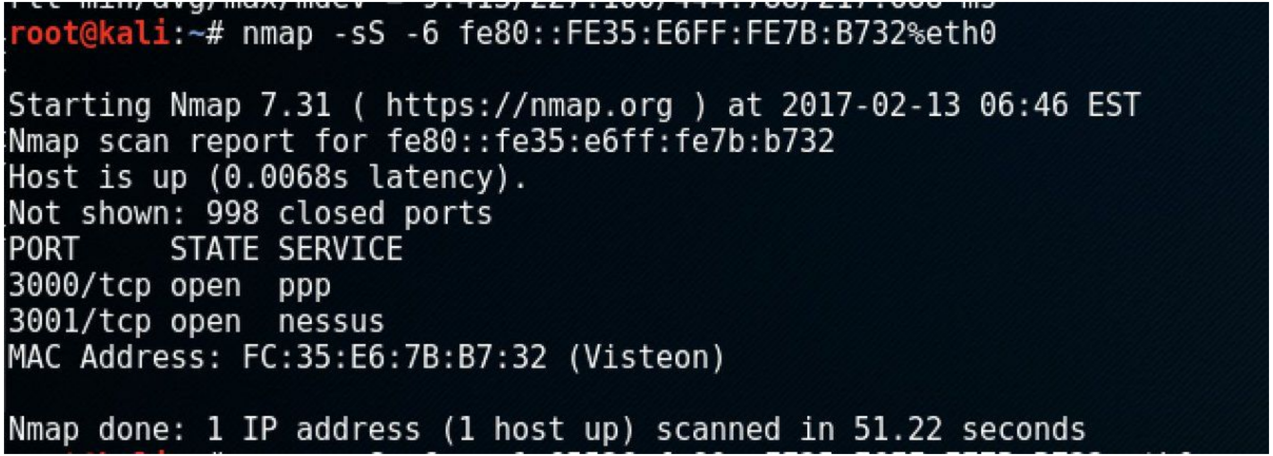
- Opening the Device





Vulnerability Scanning

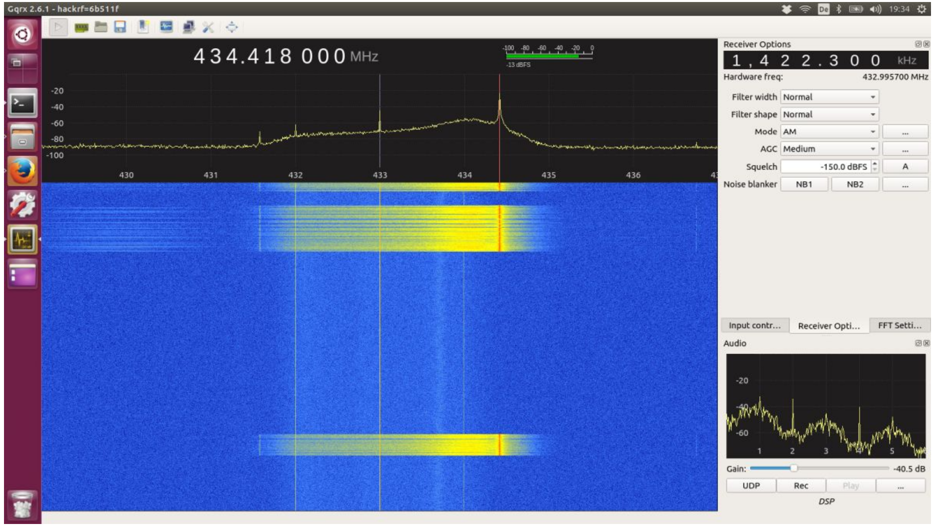
- Nessus
- Qualys
- Nmap



```
root@kali:~# nmap -sS -6 fe80::FE35:E6FF:FE7B:B732%eth0

Starting Nmap 7.31 ( https://nmap.org ) at 2017-02-13 06:46 EST
Nmap scan report for fe80::fe35:e6ff:fe7b:b732
Host is up (0.0068s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
3000/tcp open  ppp
3001/tcp open  nessus
MAC Address: FC:35:E6:7B:B7:32 (Visteon)

Nmap done: 1 IP address (1 host up) scanned in 51.22 seconds
```

Launch Attack

- DDoS
- Rolling Code
- Jamming
- RFCrack
- Attify Zigbee Framework
- HackRF One



Gqrx 2.6.1 - hackrf=6b511f

434.418 000 MHz

Receiver Options

1,422.300 kHz

Hardware freq: 432.995700 MHz

Filter width: Normal

Filter shape: Normal

Mode: AM

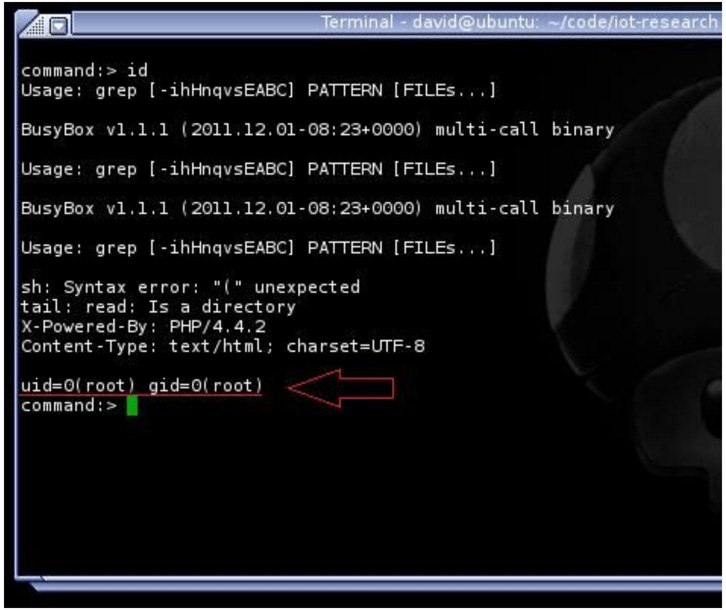
AGC: Medium

Squelch: -150.0 dBFS

Gain: -40.5 dB

Gain Access

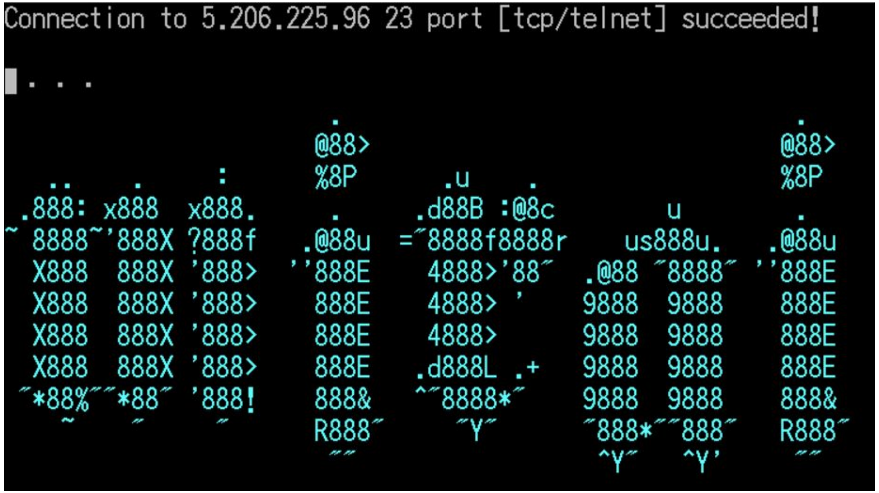
- Objective is Get Root Access
- Firmware Exploitation
- Web Vulnerabilities
- Mobile App Vulnerabilities
- Network Vulnerabilities
- UART/JTAG/USB other interfaces



```
command:> id
Usage: grep [-ihHnqvsEABC] PATTERN [FILEs...]

BusyBox v1.1.1 (2011.12.01-08:23+0000) multi-call binary

Usage: grep [-ihHnqvsEABC] PATTERN [FILEs...]

BusyBox v1.1.1 (2011.12.01-08:23+0000) multi-call binary

Usage: grep [-ihHnqvsEABC] PATTERN [FILEs...]

sh: Syntax error: "(" unexpected
tail: read: Is a directory
X-Powered-By: PHP/4.4.2
Content-Type: text/html; charset=UTF-8

uid=0(root) gid=0(root)
command:>
```

Maintain Access

- Backdoor Installation
- Physical Manipulation
- Firmware Manipulation
- Clearing Logs
- Encrypting Communication



```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

█. . .
                       .                                .
                      @88>                             @88>
   ..     .     :     %8P      .u    .                 %8P
 .888: x888  x888.     .      .d88B :@8c        u       .
~ 8888~'888X ?888f   .@88u  ="8888f8888r    us888u.   .@88u
  X888  888X '888>  ''888E    4888>'88"  .@88 "8888" ''888E
  X888  888X '888>    888E    4888> '    9888  9888    888E
  X888  888X '888>    888E    4888>      9888  9888    888E
  X888  888X '888>    888E   .d888L .+   9888  9888    888E
 "*88%""*88" '888!    888&   ^"8888*"    9888  9888    888&
   ~     "      "     R888"     "Y"      "888*""888"   R888"
                       ""                 ^Y"   ^Y'     ""
```

Securing IoT Devices

- Disable unnecessary network services
- Firmware Updates
- Block Unnecessary Ports
- Encryption in Transit (SSL/TLS)
- Encryption at Rest

Securing IoT Devices

- User Account Lockout
- Periodic Assessment of Devices
- Secure Password Recovery
- 2FA
- Disable UPnP
- Don’t forget to Secure Your Hardware

Some IoT Hacking Useful Resources

- Guides:
  - ✓ https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
  - ✓ https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf
  - ✓ https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/
  - ✓ www.youtube.com/lufsec

- Books:
  - ✓ IoT Hackers Handbook
  - ✓ IoT Penetration Testing Cookbook

- Online Courses:
  - ✓ https://www.linkedin.com/learning/ethical-hacking-hacking-iot-devices