



Hackeando Dispositivos IoT: Metodologia



Quem Sou Eu

- ❑ CISO Americas na Infineon Technologies
- ❑ Fundador da LufSec
- ❑ Autor (LinkedIn Learning)
- ❑ CISSP, CRISC, PCIP, CISM, CEH
- ❑ Amo ensinar, dar coaching, pesquisar e ler
- ❑ Voluntário DEFCON Red Team/Aviation Village
- ❑ Membro do CSA IoT Security Group



Certified in Risk
and Information
Systems Control™

Certified Information
Security Manager™
An ISACA® Certification

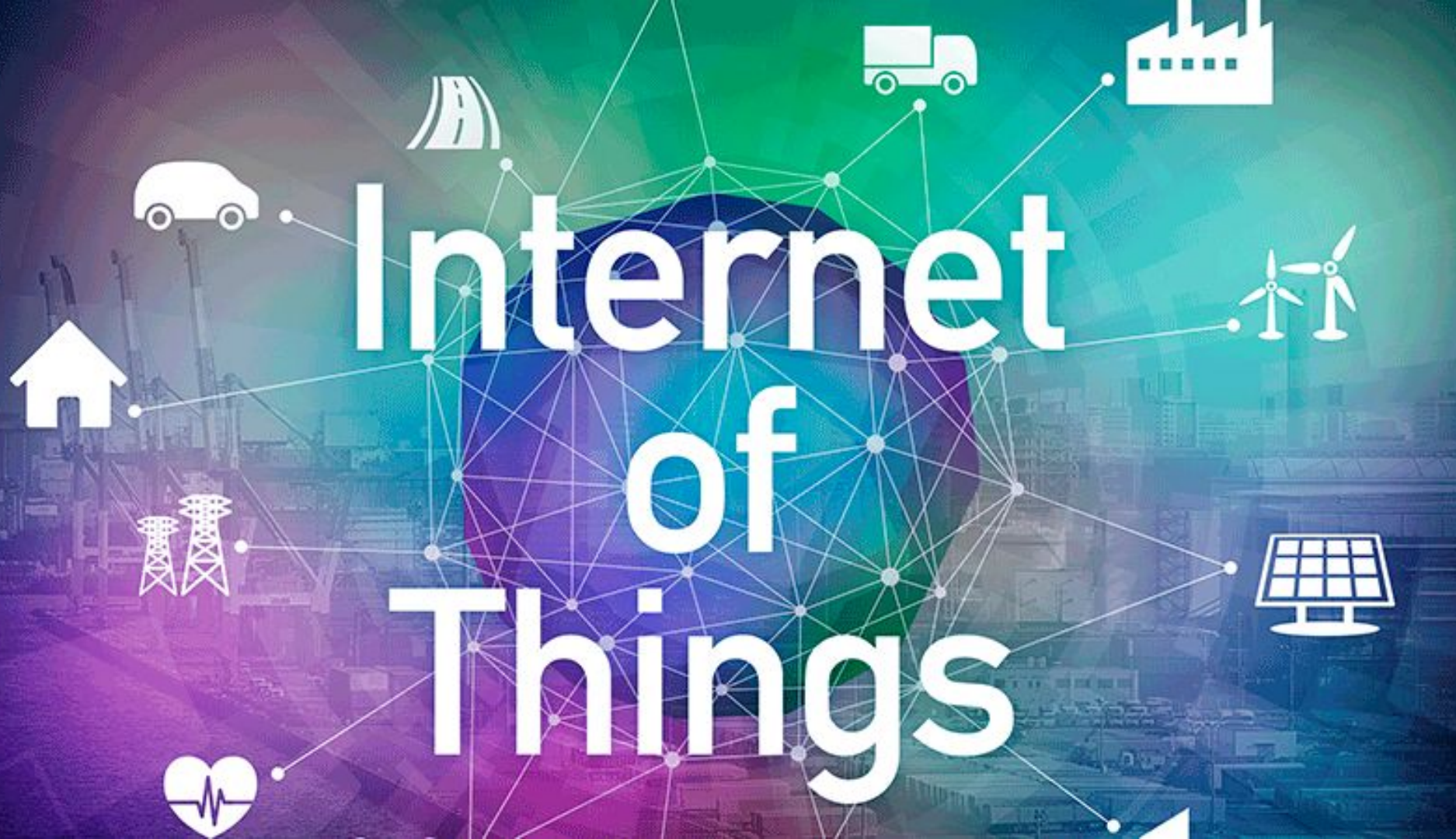
PCI PROFESSIONAL (PCIP)™
PROGRAM

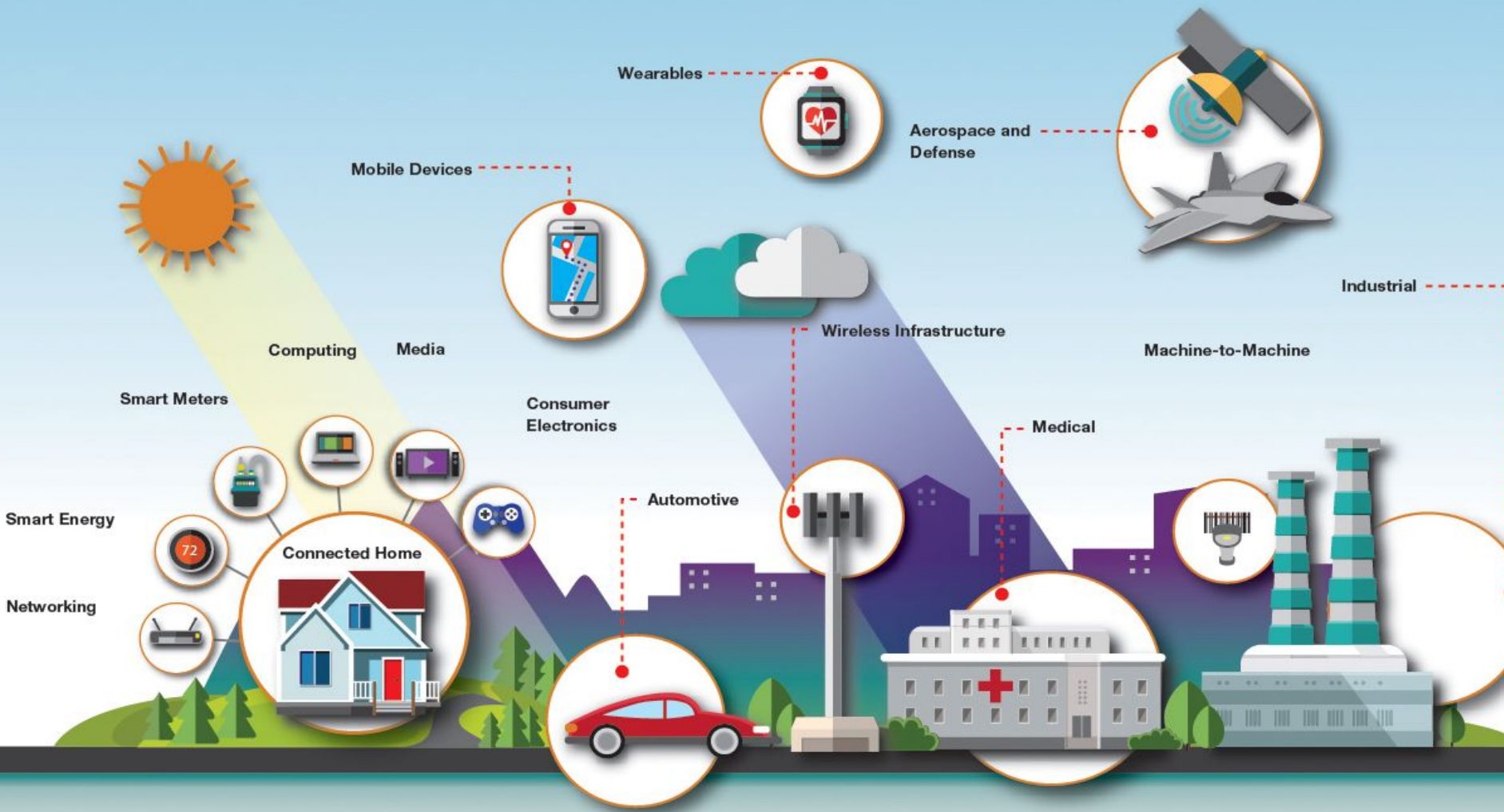
Certified Ethical Hacker

Aviso Legal

As opiniões expressas nesta apresentação são do autor e não refletem a política ou posição oficial da Infineon Technologies

Internet of Things





Segurança em IoT: De Volta para 1991?

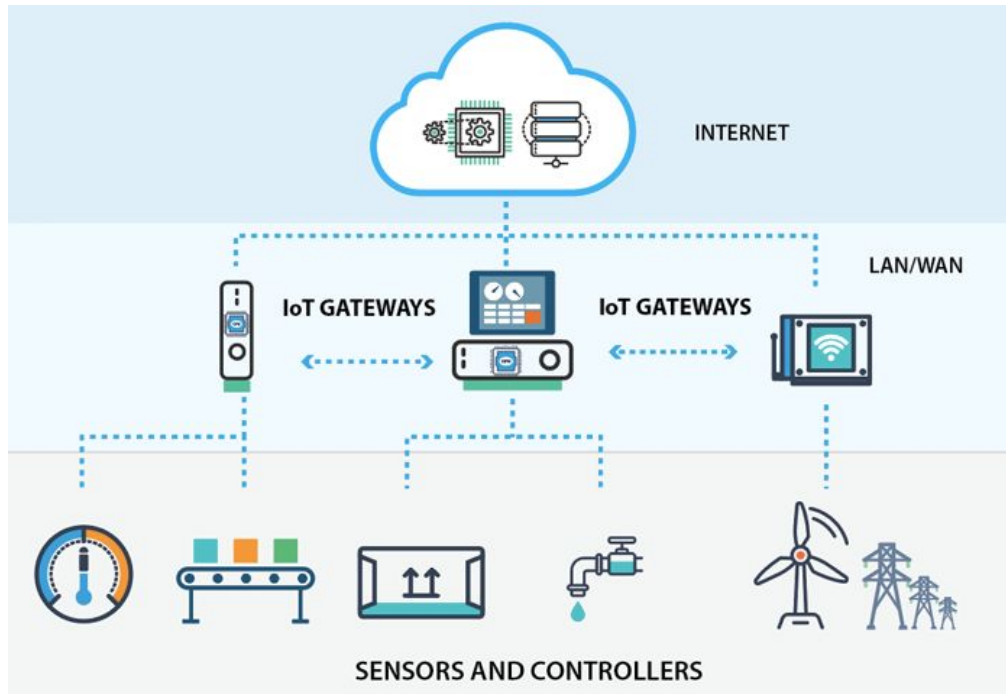


Por que Pentest em Dispositivos IoT

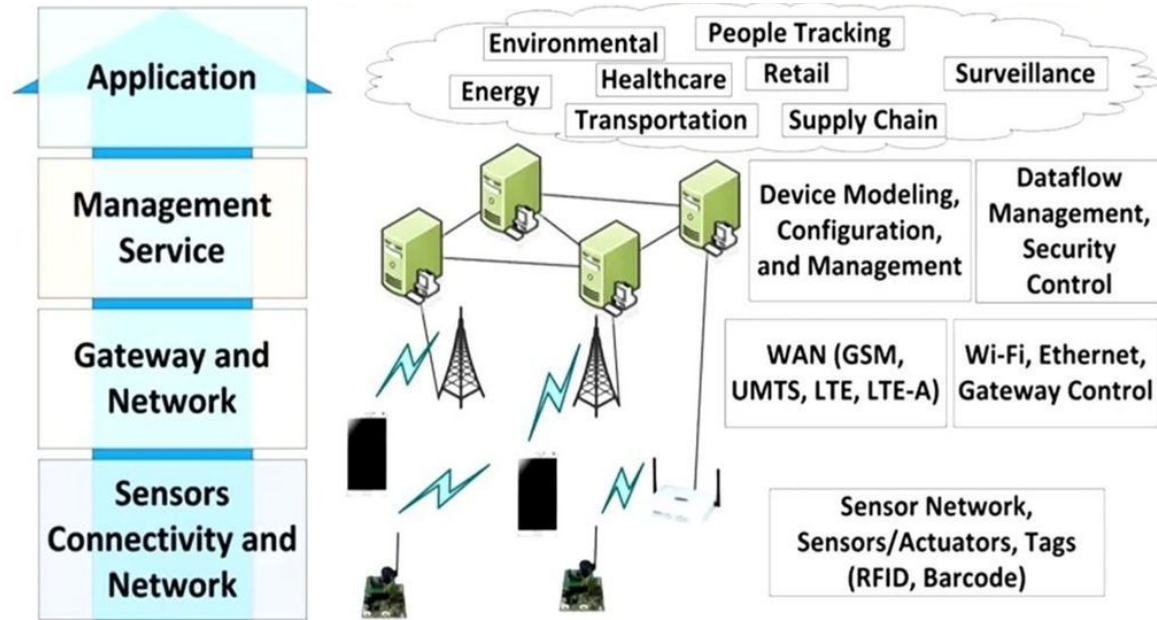
- Entender os riscos que os dispositivos IoT trazem para a organização
- Participar em programas de Bug Bounties
- Segurança de Produto
- Desafiar a si mesmo
- Pegar esse "Momentum"

Conexão com a Internet em IoT

- Cabo
- Sem Fio
- Gateway



Camadas de Arquitetura em IoT



Tecnologias e Protocolos usados em IoT

Comunicação Sem Fio			Comunicação Cabeada	Sistemas Operacionais
Curta Distancia	Media Distancia	Longa Distancia		
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

Desafios de Segurança em IoT



Desafios de Segurança em IoT

- Entender como o dispositivo funciona (opera, se comunica)
- Problemas de Interoperabilidade (soluções proprietárias)
- Atualizações de Firmware Ineficientes ou Inexistentes
- Interfaces Vulneráveis (Interfaces Web, APIs)
- Proteção de segurança física ineficiente (backdoors)
- Suporte do Fornecedor Insuficiente



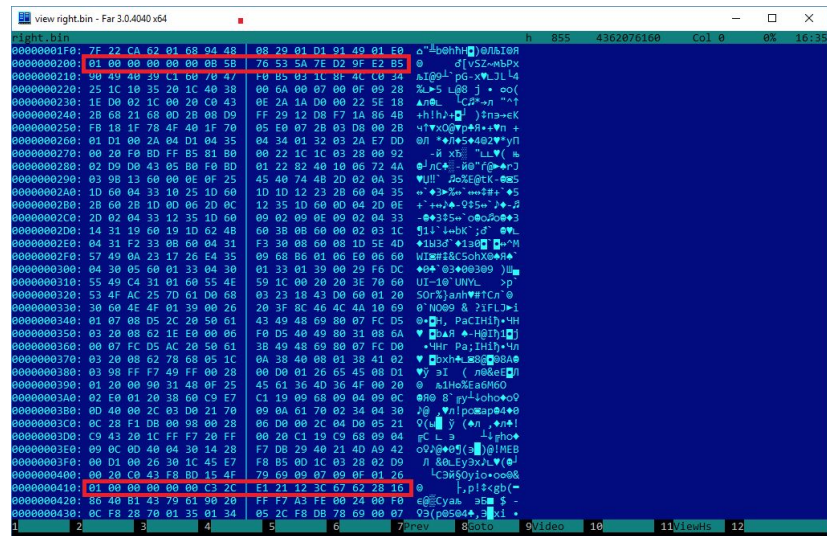
OWASP IoT Top 10

1. Senhas Fracas, fáceis de adivinhar ou Hardcoded
2. Serviços de Rede Não Seguros
3. Interfaces de Ecossistemas Inseguros
4. Mecanismos de atualização inexistentes ou inseguros
5. Uso de Componentes Inseguros ou Desatualizados
6. Proteções de Privacidade Insuficientes
7. Armazenamento ou Transmissão de Dados Insegura
8. Falta de Gerenciamento de Dispositivo
9. Configurações de Fábrica Inseguras
10. Segurança Física Ineficiente



Superfície de Ataque em IoT

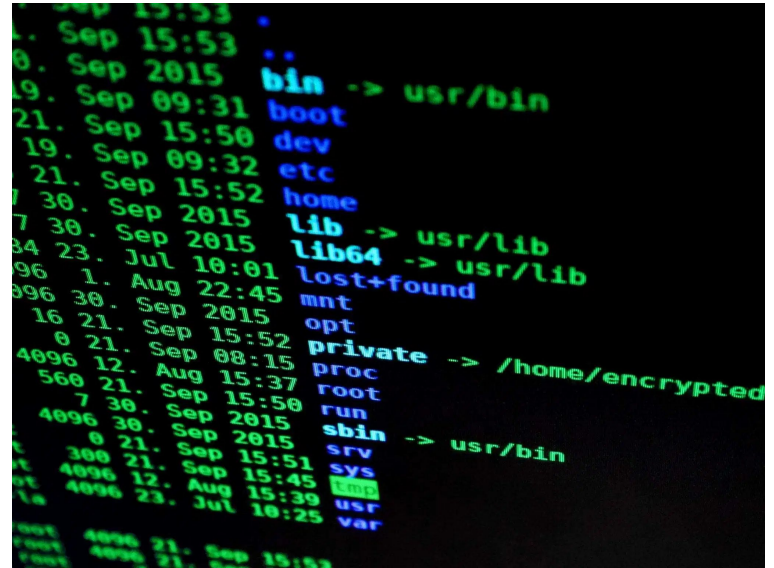
- Memória dos Dispositivos contendo credenciais
- Resetar para um estado inseguro
- Controle de Acesso
- Extração de Firmware
- Escalonamento de Privilégios
- Ataques Web
- Ataques de Firmware



The image shows a hex editor window titled 'view right.bin - Far 3.0.4040 v64'. The main area displays hexadecimal data in columns, with corresponding ASCII characters on the right. Several lines of data are highlighted in red, indicating specific memory locations. The ASCII column contains various characters, including spaces, punctuation, and some symbols, which may represent sensitive information like credentials or control sequences.

Superfície de Ataque em IoT

- Ataques em Serviços de Rede
- Dados não criptografados
- Confidencialidade e Integridade
- Ataques em Sistemas na Nuvem
- Atualizações Maliciosas
- APIs Não Seguras
- Aplicações de Celular



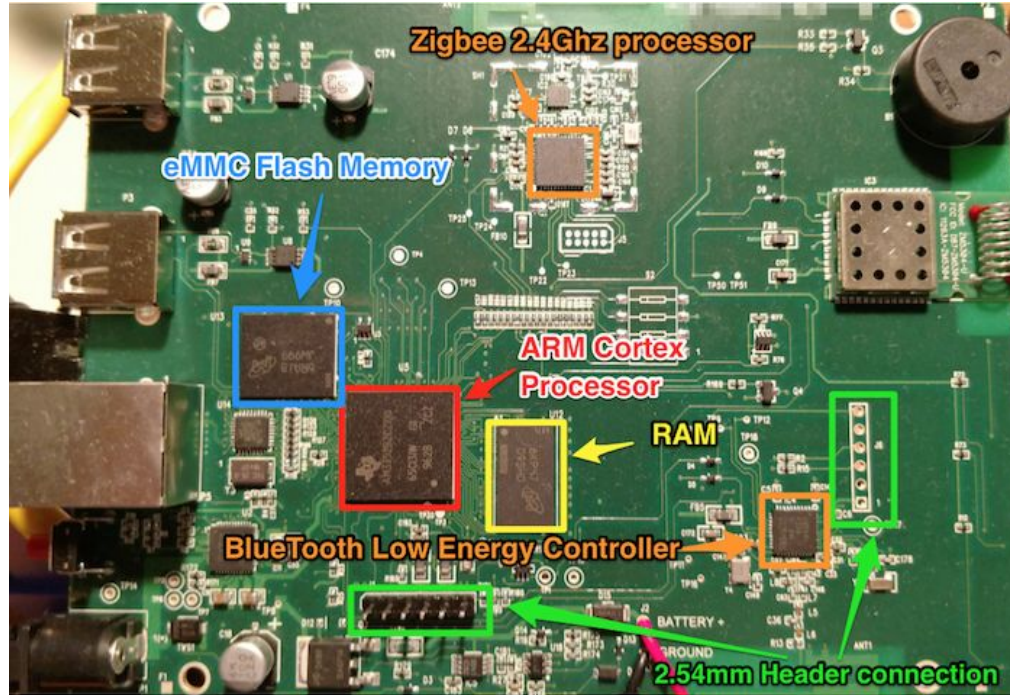
Ataques Comuns em IoT

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

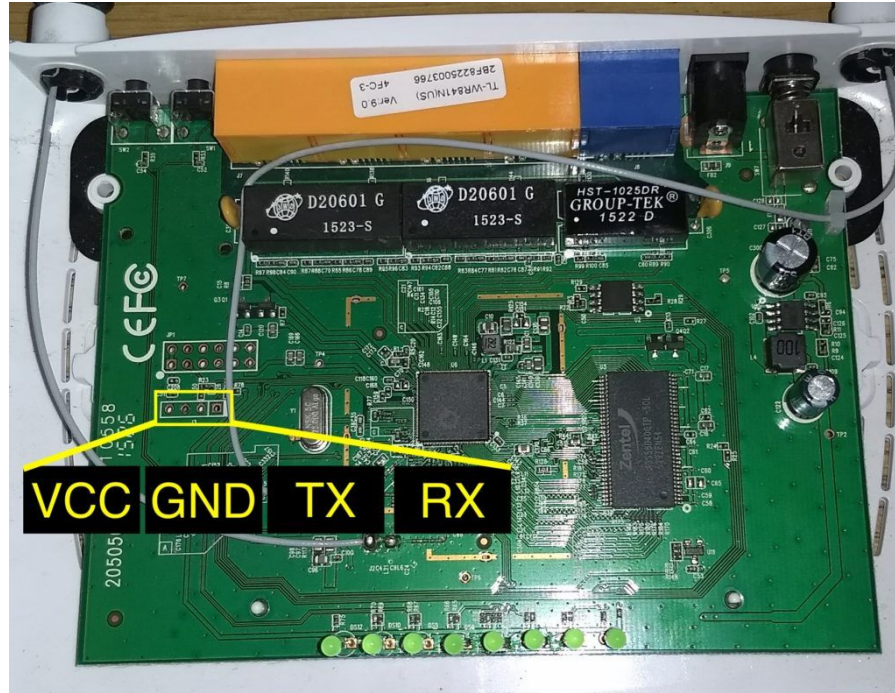
Ataques Comuns em IoT

- Sybil
- Exploit Kits
- Man-in-the-Middle
- Forged Malicious Devices
- Side-channel (Spectre/Meltdown)
- Ransomware

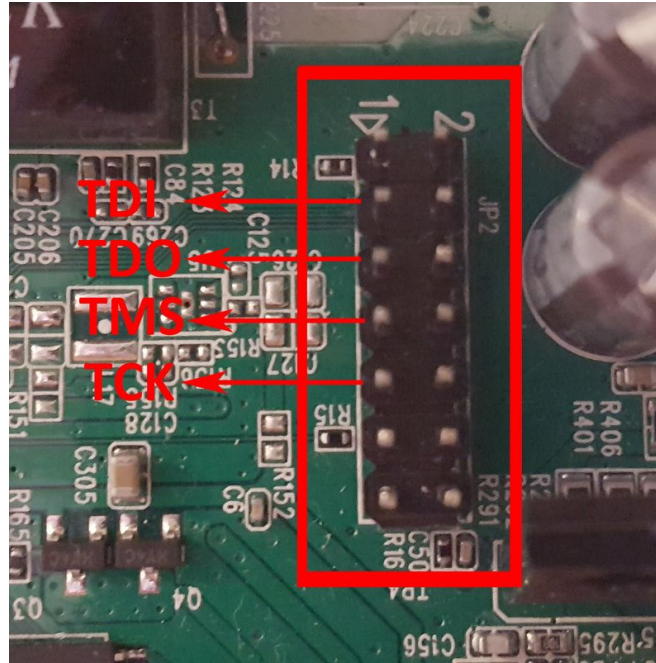
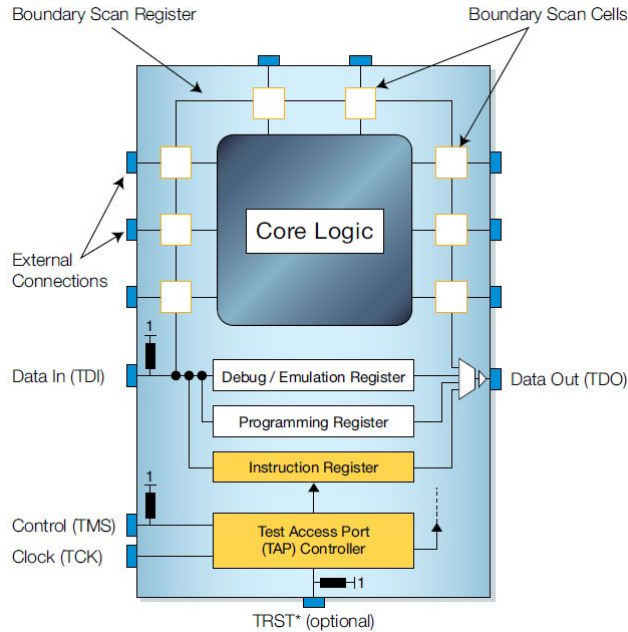
Componentes de Hardware



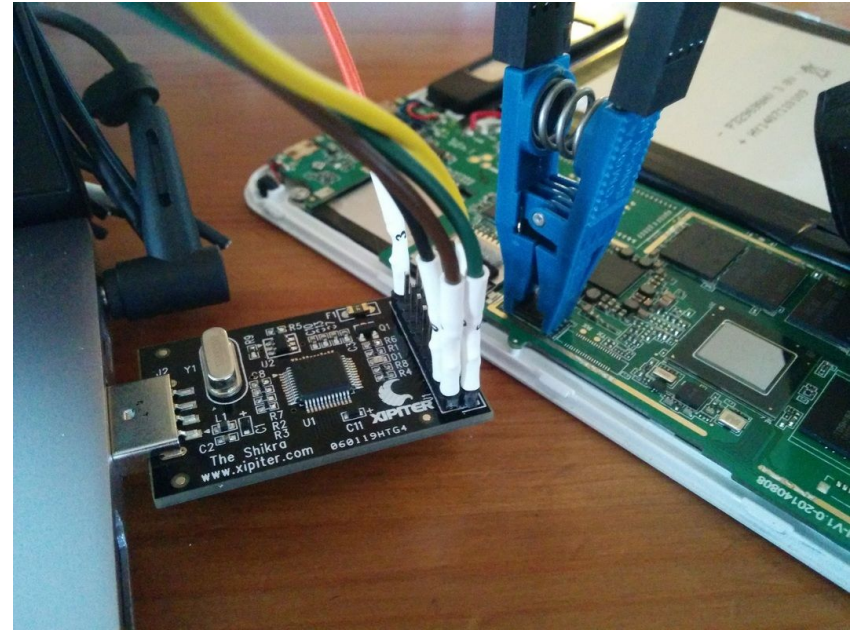
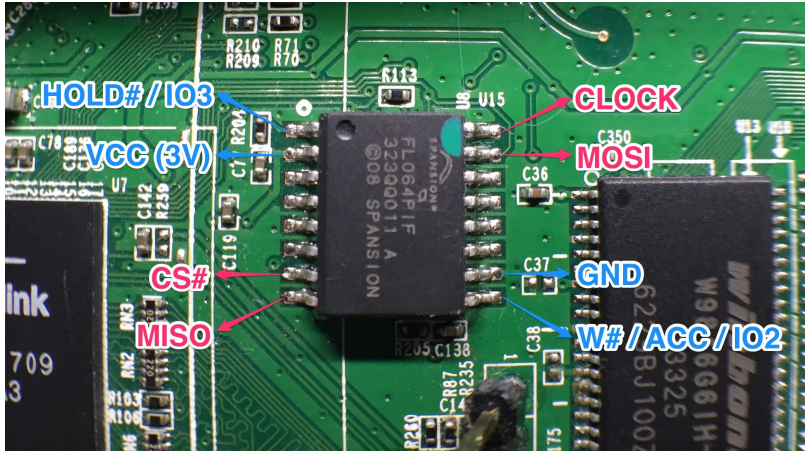
Componentes de Hardware - UART



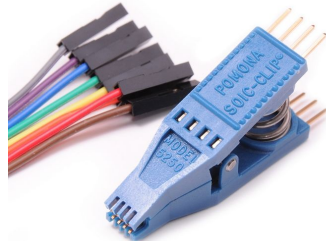
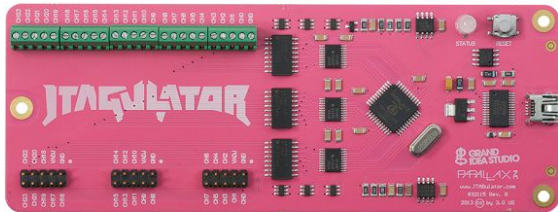
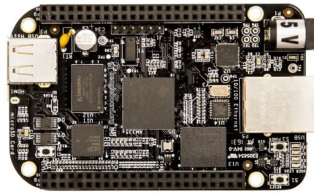
Componentes de Hardware - JTAG



Componentes de Hardware - SPI



Ferramentas Úteis - Hackear IoT



Plataformas SO para IoT Hacking

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



Ferramentas de Frameworks

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



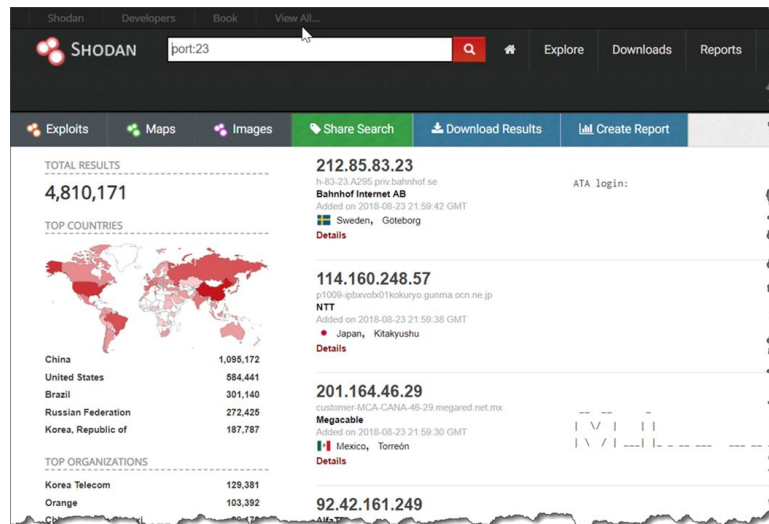
IoT Hacking: Metodologia

- Reconhecimento
- Escaneamento
- Efetuando o Ataque
- Obtendo Acesso
- Mantendo Acesso



Reconhecimento

- Entender Como o Dispositivo Funciona/Opera
- FCC ID/Anatel
- Manuais e Datasheets
- Shodan
- Endereços IP
- Protocolos Utilizados
- Página Web do Fabricante



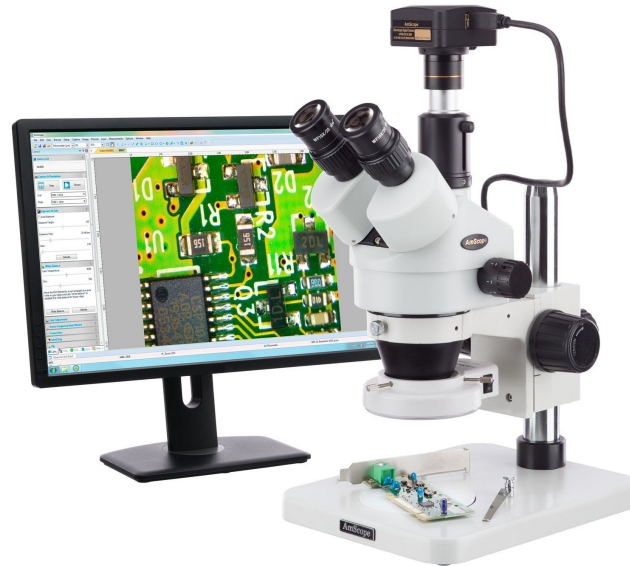
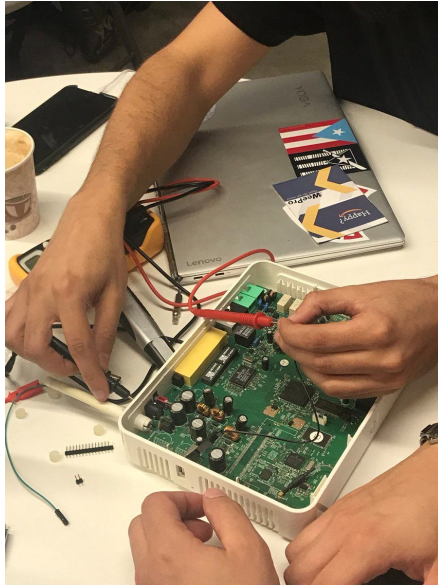
The screenshot displays the Shodan search engine interface. The search bar contains the query 'port:23'. The results page shows a total of 4,810,171 results. A world map highlights the top countries, with China having the highest number of results at 1,095,172. The top organizations listed are Korea Telecom (129,381) and Orange (103,392). The interface also features a navigation menu with options like 'Exploits', 'Maps', 'Images', 'Share Search', 'Download Results', and 'Create Report'. On the right side, there are three detailed search results for IP addresses: 212.85.83.23 (Bahnhof Internet AB), 114.160.248.57 (NTT), and 201.164.46.29 (Megacable).

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

Organization	Count
Korea Telecom	129,381
Orange	103,392

Reconhecimento

- Abrindo o Dispositivo



Escaneamento

- Nessus
- Qualys
- Nmap

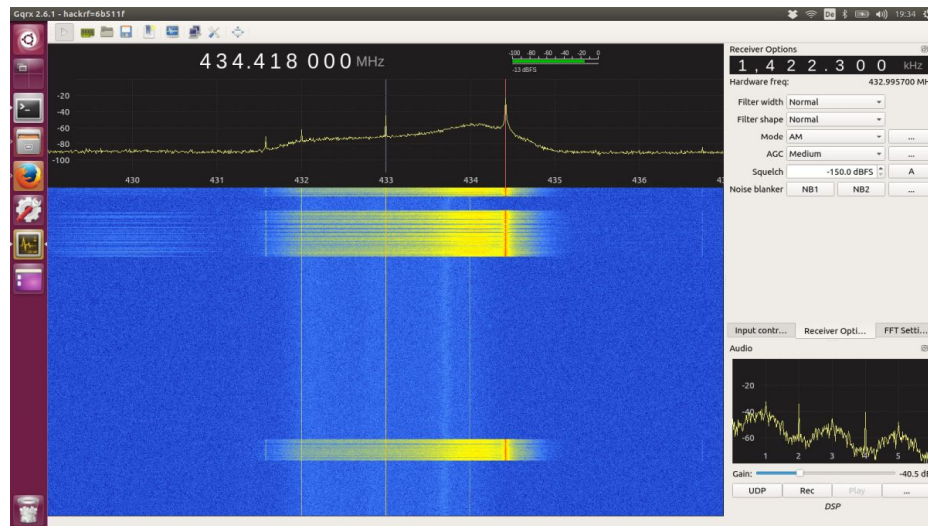
```
root@kali:~# nmap -sS -6 fe80::FE35:E6FF:FE7B:B732%eth0

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
```

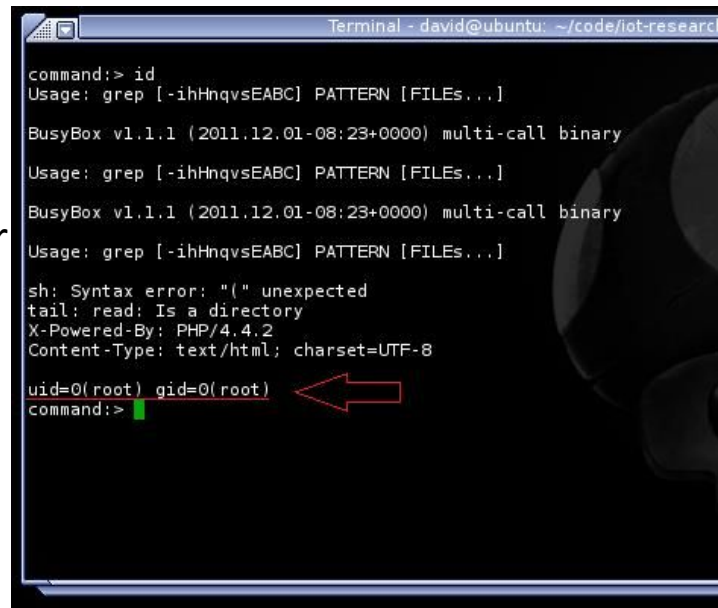

Lançando os Ataques

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



Ganhando Acesso

- Objetivo é Ganhar Acesso Root
- Exploração de Firmware
- Vulnerabilidades Web
- Vulnerabilidades em Aplicativos de Celular
- Vulnerabilidades de Rede
- UART/JTAG/USB e outras interfaces



```
Terminal - david@ubuntu: ~/code/iot-research
command:> id
Usage: grep [-iHhqvseABC] PATTERN [FILEs...]

BusyBox v1.1.1 (2011.12.01-08:23+0000) multi-call binary
Usage: grep [-iHhqvseABC] PATTERN [FILEs...]

BusyBox v1.1.1 (2011.12.01-08:23+0000) multi-call binary
Usage: grep [-iHhqvseABC] 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:>
```

Mantendo Acesso

- Instalação de Backdoor
- Manipulação Física
- Manipulação de Firmware
- Limpando Logs
- Criptografando Comunicações

```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!  
.....  
@88> @88>  
%8P %8P  
      .u      .  
      :      :  
      .888: x888 x888.      .d88B :@8c      u      @88u  
~ 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~      ^V~      ^V~      ^V~      ^V~  
      ^V~      ^V~      ^V~      ^V~
```

Segurança em Dispositivos IoT

- Desabilitando serviços de rede desnecessários
- Atualizações de Firmware
- Bloqueando Portas Desnecessárias
- Criptografia em Trânsito (SSL/TLS)
- Criptografia em Repouso



Segurança em Dispositivos IoT

- Bloqueio de Conta de Usuário
- Testar Segurança dos Dispositivos Periodicamente
- Recuperação de Senha Segura
- Autenticação de 2 Fatores
- Desabilitar UPnP
- Não se esqueça da Segurança Física



Mais Informações sobre IoT Hacking

- Guias:
 - ✓ 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
- Livros:
 - ✓ IoT Hackers Handbook
 - ✓ IoT Penetration Testing Cookbook
- Cursos Online:
 - ✓ <https://www.linkedin.com/learning/ethical-hacking-hacking-iot-devices>

Informações para Contato

-  @lucianoferrari
-  [linkedin.com/in/lucianoferrari](https://www.linkedin.com/in/lucianoferrari)
-  www.lufsec.com
-  lferrari@lufsec.com
-  github.com/lucianoferrari
-  [youtube.com/lufsec](https://www.youtube.com/lufsec)