



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -
SECURITY IMPLEMENTATION

Progresso do curso

Módulo 16. Hacking Wireless Networks

Módulo 17. Hacking Mobile Applications

Módulo 18. IoT & OT Hacking

Módulo 19. Cloud Computing

Módulo 20. Cryptography

Conceitos sobre IoT:

O IoT é um tópico importante e emergente no campo da tecnologia, economia e sociedade em geral. É conhecida como a teia de dispositivos conectados, possibilitada pela interseção entre as comunicações máquina a máquina e a análise de big data. O IoT é um desenvolvimento voltado para o futuro da Internet e das capacidades dos dispositivos físicos que estão gradualmente estreitando a lacuna entre o mundo virtual e físico.



CEHv12

18.IoT & OT Hacking



Objetivos

O principal objetivo deste módulo é explicar as potenciais ameaças para as plataformas IoT e OT e fornecer orientações para proteger os dispositivos IoT e a infraestrutura OT de ameaças e ataques em evolução.

No final deste módulo, você será capaz de

- ☐ Explicar os conceitos de IoT e OT
- ☐ Compreender diferentes ameaças e ataques de IoT e OT
- ☐ Descrever a metodologia de hacking IoT e OT
- ☐ Aplicar contramedidas para proteger os dispositivos de ataques IoT e OT

Introdução

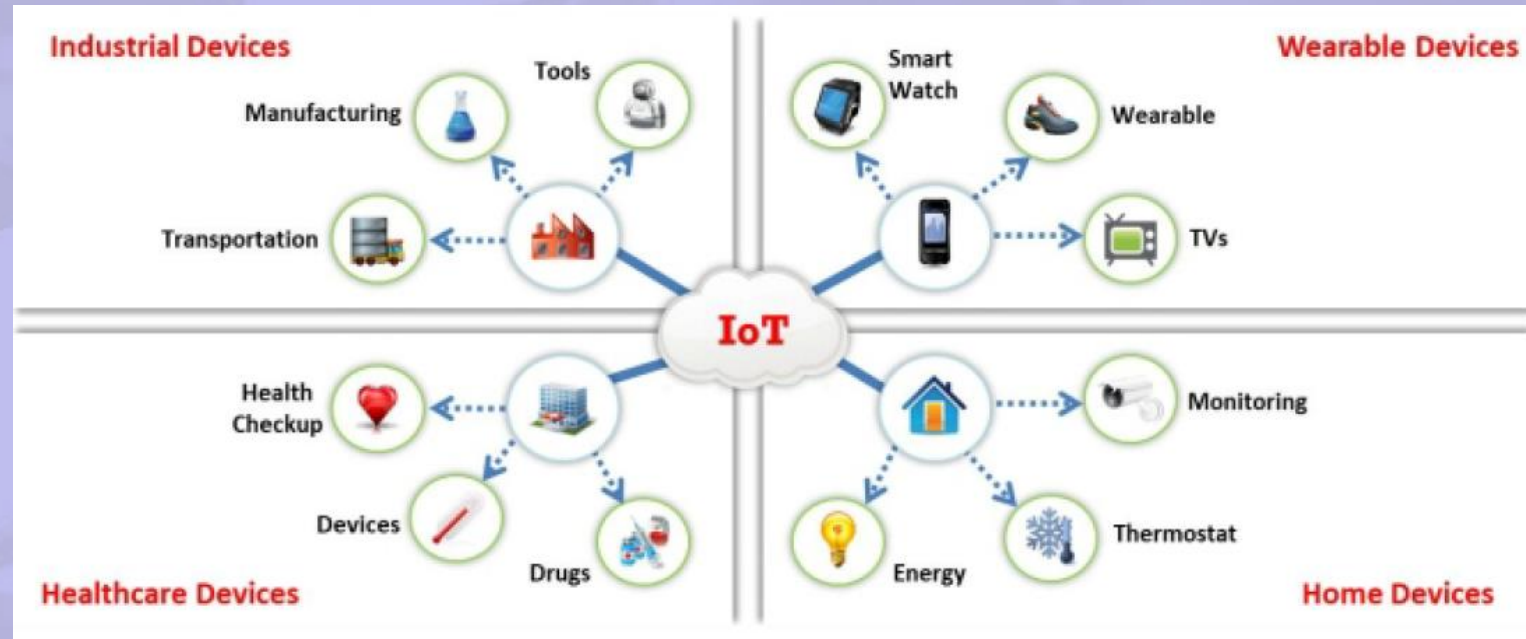
A Internet das Coisas (IoT) evoluiu a partir da convergência da tecnologia sem fio, sistemas micro eletromecânicos, micros serviços e Internet. As soluções de IoT são aplicadas em diferentes setores da indústria, incluindo saúde, gerenciamento de edifícios, agricultura, energia e transporte. Muitas organizações estão conduzindo a transformação da IoT. Dispositivos IoT, como *wearables, aparelhos industriais, dispositivos eletrônicos conectados, redes inteligentes e veículos inteligentes, estão se tornando parte de redes interconectadas. Esses dispositivos geram uma grande quantidade de dados que são coletados, analisados, registrados e armazenados nas redes.

- “wearable technology” ou “tecnologias vestíveis”. A tradução direta para o português pode até parecer um pouco limitada ou estranha, uma vez que a categoria ainda está expandindo os seus horizontes. Entretanto, no que depender da indústria, os investimentos nesse segmento só tendem a aumentar.

Fonte: <https://www.tecmundo.com.br/tecnologia/49699-wearables-sera-que-esta-moda-pegar-.htm>

O que é IoT

- A Internet das Coisas (IoT), também conhecida como Internet de Todas as Coisas (IoE), refere-se a dispositivos de computação que são habilitados para a web e têm a capacidade de detectar, coletar e enviar dados usando sensores e o hardware de comunicação e processadores que estão embutidos no dispositivo. Na IoT, uma "coisa" refere-se a um dispositivo implantado em um objeto natural, feito pelo homem ou por uma máquina e tem a funcionalidade de se comunicar por meio de uma rede.

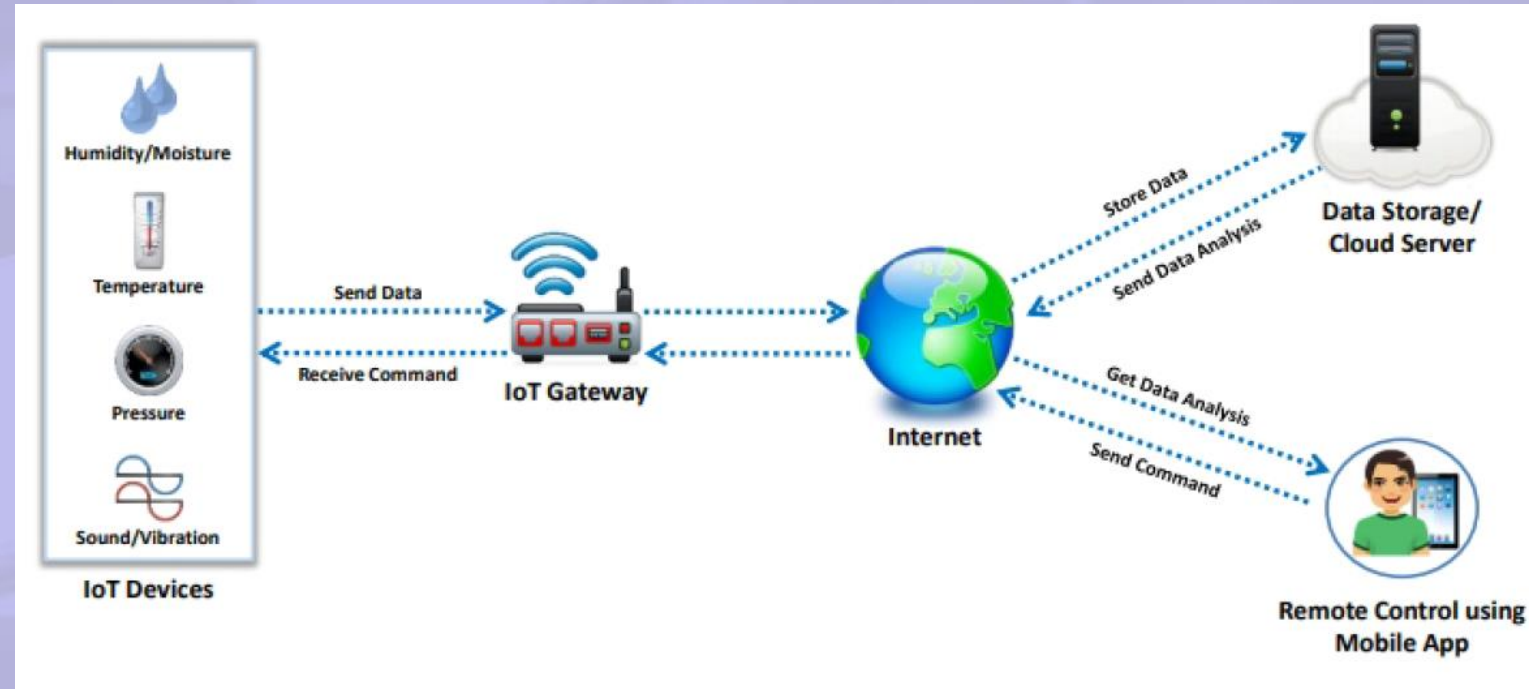


Como funciona o IoT

- A tecnologia IoT inclui quatro sistemas principais:

1. Dispositivos IoT
2. Sistemas de gateway
3. Sistemas de armazenamento de dados usando tecnologia de nuvem
4. Controle remoto usando aplicativos móveis.

- Esses sistemas juntos tornam possível a comunicação entre dois terminais.



IoT – Protocolos e Tecnologias

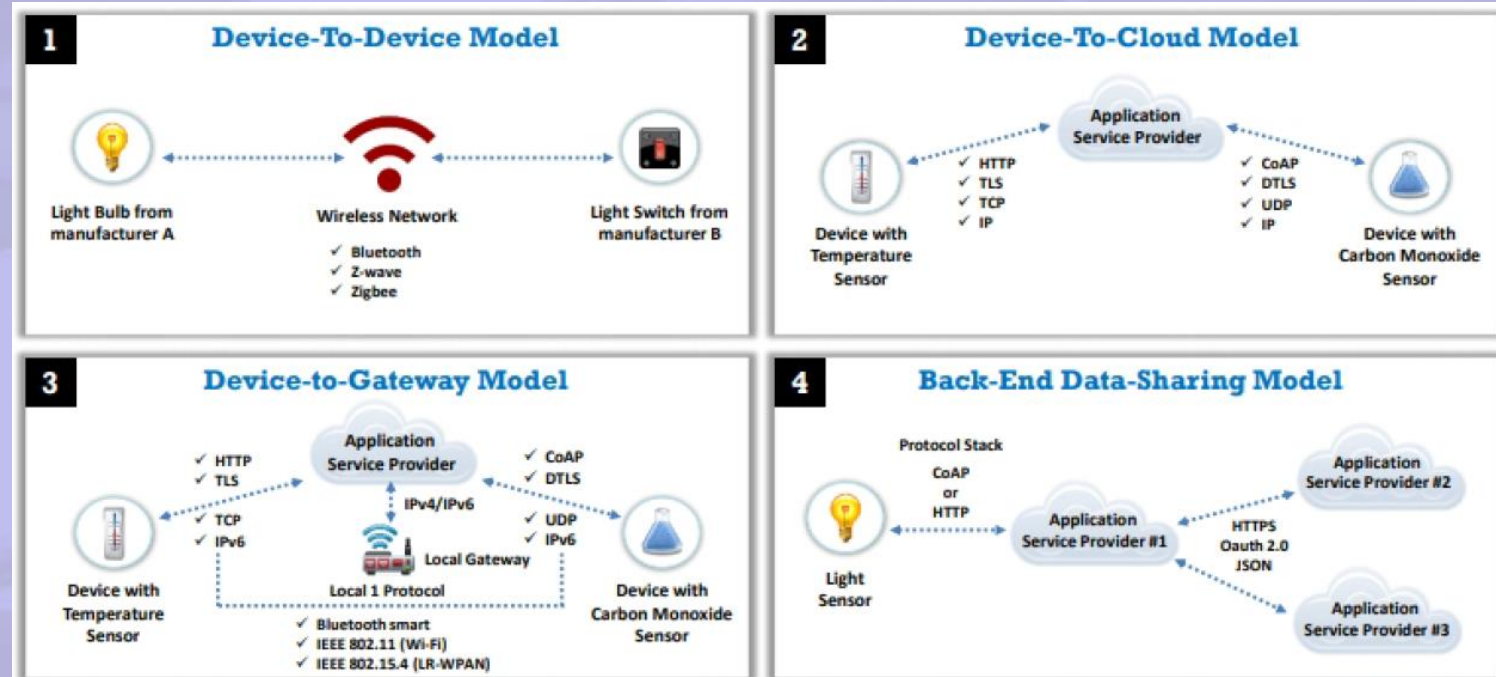
- A IoT inclui uma ampla gama de novas tecnologias e habilidades. O desafio no espaço do IoT é a imaturidade das tecnologias com serviços associados e dos fornecedores que os fornecem. Isso representa um desafio importante para as organizações que exploram o IoT. Para uma comunicação bem-sucedida entre dois terminais, a IoT implementa principalmente protocolos padrão e de rede.

IoT Technologies and Protocols

Short-range Wireless Communication	Medium-range Wireless Communication	Long-range Wireless Communication	IoT Operating Systems	IoT Application Protocols
<ul style="list-style-type: none">Bluetooth Low Energy (BLE)Light-Fidelity (Li-Fi)Near Field Communication (NFC)QR Codes and BarcodesRadio Frequency Identification (RFID)ThreadWi-fiWi-Fi DirectZ-waveZigBeeANT	<ul style="list-style-type: none">Ha-LowLTE-Advanced6LoWPANQUIC <p>Wired Communication</p> <ul style="list-style-type: none">EthernetMultimedia over Coax Alliance (MoCA)Power-line Communication (PLC)	<ul style="list-style-type: none">Low-power Wide-area Networking (LPWAN)<ul style="list-style-type: none">LoRaWANSigfoxNeulVery Small Aperture Terminal (VSAT)CellularMQTTNB-IoT	<ul style="list-style-type: none">Windows 10 IoTAmazon FreeRTOSContikiFuchsiaRIOTUbuntu CoreARM mbed OSZephyrNucleus RTOSNuttX RTOSIntegrity RTOS	<ul style="list-style-type: none">CoAPEdgeLWM2MPhysical WebXMPPMihini/M3DA

Modelos de Comunicação

- A tecnologia IoT usa vários modelos de comunicação, cada um com suas próprias características.
- Esses modelos destacam a flexibilidade com a qual os dispositivos IoT podem se comunicar entre si ou com o cliente.



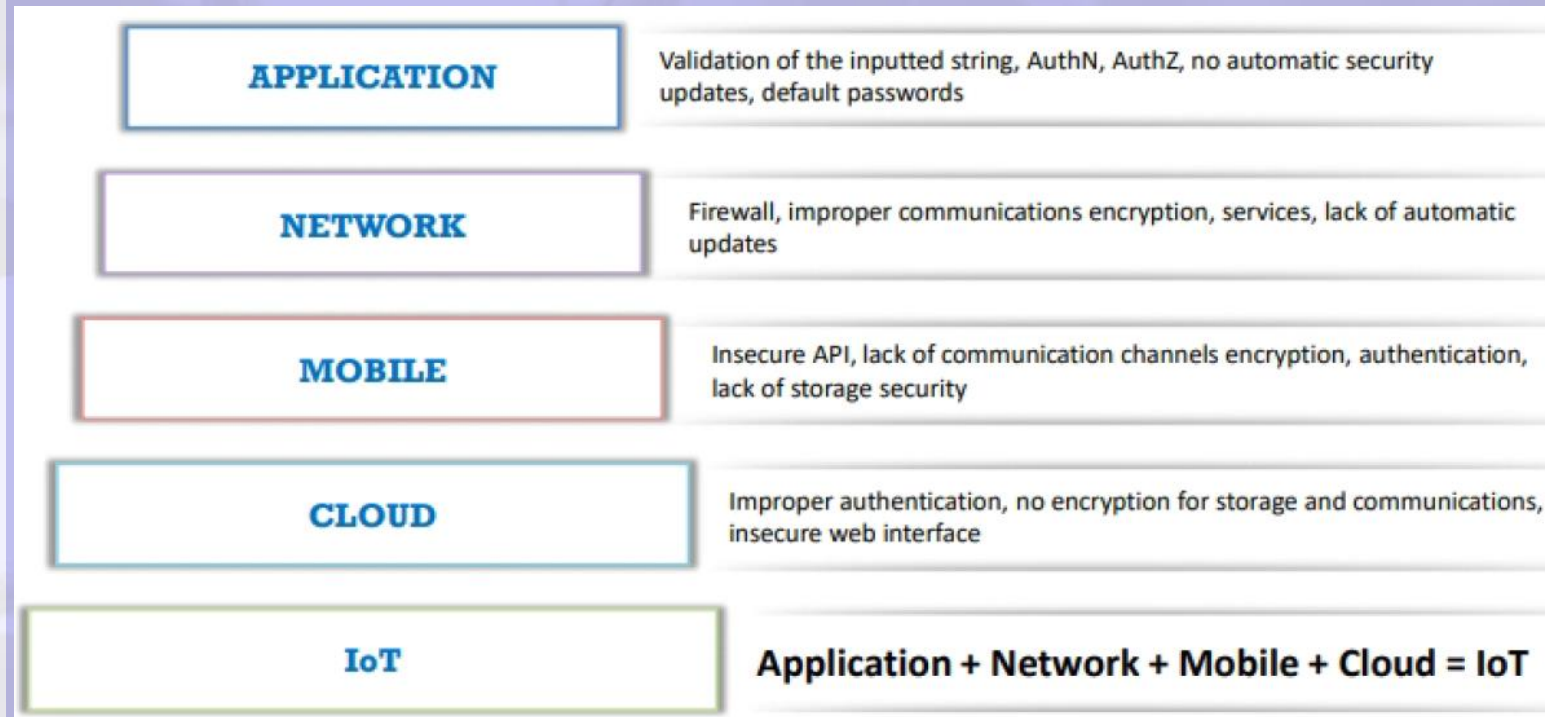
Desafios de IoT

- A tecnologia IoT está crescendo tão rapidamente que se tornou onipresente. Com vários aplicativos e recursos; mas faltam políticas básicas de segurança, os dispositivos IoT são atualmente presas fáceis para os hackers. As atualizações para dispositivos IoT introduziram novas falhas de segurança que podem ser facilmente exploradas por hackers.

01	Lack of security and privacy	05	Clear text protocols and unnecessary open ports	09	Interoperability standard issues
02	Vulnerable web interfaces	06	Coding errors (buffer overflow)	10	Physical theft and tampering
03	Legal, regulatory, and rights issues	07	Storage issues	11	Lack of vendor support for fixing vulnerabilities
04	Default, weak, and hardcoded credentials	08	Difficult to update firmware and OS	12	Emerging economy and development issues

Problemas de segurança de IoT

- Vulnerabilidades no sistema IoT podem resultar em grandes problemas para as organizações. A maioria dos dispositivos IoT vem com problemas de segurança, como a ausência de um mecanismo de autenticação adequado ou o uso de credenciais padrão, ausência de um mecanismo de bloqueio, ausência de um esquema de criptografia forte, ausência de sistemas de gerenciamento de chaves adequados e segurança física.



OWASP Top 10 IoT

1

Weak, Guessable, or Hardcoded Passwords

2

Insecure Network Services

3

Insecure Ecosystem Interfaces

4

Lack of Secure Update Mechanisms

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


Vulnerabilidades do IoT

Vulnerability	Description	Vulnerabilities	Obstacles
1. Username Enumeration	<ul style="list-style-type: none"> Ability to collect a set of valid usernames by interacting with the authentication mechanism 	10. Removal of Storage Media	<ul style="list-style-type: none"> Ability to physically remove the storage media from the device
2. Weak Passwords	<ul style="list-style-type: none"> Ability to set account passwords to '1234' or '123456' for example Usage of pre-programmed default passwords 	11. No Manual Update Mechanism	<ul style="list-style-type: none"> No ability to manually force an update check for the device
3. Account Lockout	<ul style="list-style-type: none"> Ability to continue sending authentication attempts after 3 - 5 failed login attempts 	12. Missing Update Mechanism	<ul style="list-style-type: none"> No ability to update the device
4. Unencrypted Services	<ul style="list-style-type: none"> Network services are not properly encrypted to prevent eavesdropping or tampering by attackers 	13. Firmware Version Display and/or Last Update Date	<ul style="list-style-type: none"> Current firmware version is not displayed and/or the last update date is not displayed
5. Two-factor Authentication	<ul style="list-style-type: none"> Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner 	14. Firmware and Storage Extraction	<ul style="list-style-type: none"> Firmware contains a lot of useful information, like source code and binaries of running services, pre-set passwords, and ssh keys
6. Poorly Implemented Encryption	<ul style="list-style-type: none"> Encryption is implemented but is improperly configured or not being properly updated, e.g. using SSL v2 	15. Manipulating the Code Execution Flow of the Device	<ul style="list-style-type: none"> With the help of a JTAG adapter and GNU debugger, we can modify the execution of firmware in the device and bypass almost all software-based security controls Side channel attacks can modify the execution flow or can be used to leak information from the device
7. Update Sent Without Encryption	<ul style="list-style-type: none"> Updates are transmitted over the network without using TLS or encrypting the update file itself 	16. Obtaining Console Access	<ul style="list-style-type: none"> By connecting to a serial interface, we can obtain full console access to a device Usually security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed.
8. Update Location Writable	<ul style="list-style-type: none"> Storage location for update files is world writable, which can allow firmware to be modified and distributed to all users 	17. Insecure Third-party Components	<ul style="list-style-type: none"> Out of date versions of busybox, openssl, ssh, web servers, etc.
9. Denial of Service	<ul style="list-style-type: none"> Service can be attacked in a way that denies service to that service or the entire device 		

<https://www.owasp.org>

Ameaças do IoT

- Os dispositivos IoT têm poucos mecanismos de proteção de segurança contra várias ameaças emergentes. Esses dispositivos podem ser infectados por malware ou código malicioso em uma taxa alarmante. Os invasores costumam explorar esses dispositivos mal protegidos na Internet para causar danos físicos à rede, grampear a comunicação e também lançar ataques disruptivos, como DDoS.

01	DDoS Attack	08	Sybil Attack	15	Client Impersonation
02	Attack on HVAC Systems	09	Exploit Kits	16	SQL Injection Attack
03	Rolling Code Attack	10	Man-in-the-Middle Attack	17	SDR-Based Attack
04	BlueBorne Attack	11	Replay Attack	18	Fault Injection Attack
05	Jamming Attack	12	Forged Malicious Device	19	Network Pivoting
06	Remote Access using Backdoor	13	Side Channel Attack	20	DNS Rebinding Attack
07	Remote Access using Telnet	14	Ransomware		

Outros tipos de ataques ao IoT

Sybil Attack	☐ The attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks
Exploit Kits	☐ The attacker uses malicious script to exploit poorly patched vulnerabilities in an IoT device
Man-in-the-Middle Attack	☐ The attacker pretends to be a legitimate sender who intercepts all the communication between the sender and receiver, and hijacks the communication
Replay Attack	☐ The attacker intercepts legitimate messages from a valid communication and continuously sends the intercepted message to the target device to perform a denial-of-service attack or crash the target device
Forged Malicious Device	☐ The attacker replaces authentic IoT devices with malicious devices, if they have physical access to the network
Side-Channel Attack	☐ The attacker extracts information about encryption keys by observing the emission of signals i.e. "side channels" from IoT devices
Ransomware Attack	☐ Ransomware is a type of malware that uses encryption to block the user's access to his/her device either by locking the screen or by locking the user's files

Metodologia de IoT Hacking

- Usando a metodologia de hacking da IoT, um invasor adquire informações por meio de técnicas como coleta de informações, identificação da área de superfície de ataque e varredura de vulnerabilidade e as usa para hackear o dispositivo e a rede alvo.

IoT Hacking Methodology

Information Gathering	The first step in IoT device hacking is to extract information such as IP address, protocols used, open ports, device type, geo location of a device, manufacturing number, and manufacturing company of a device
Vulnerability Scanning	Vulnerability scanning helps an attacker to identify the IoT devices with weak configurations such as hidden exploits, firmware bugs, weak settings and passwords, and poorly encrypted communications
Launch Attacks	The vulnerabilities found are exploited further to launch various attacks such as DoS attacks, rolling code attacks, jamming signal attacks, Sybil attacks, MITM attacks, data and identity theft attacks
Gain Remote Access	Based on the vulnerabilities in an IoT device, the attacker may turn the device into a backdoor to gain access to an organization's network without infecting any end system that is protected by IDS/IPS, firewall, antivirus software, etc.
Maintain Access	Attackers remain undetected by clearing the logs , update the firmware and use malicious programs such as backdoors and Trojans to maintain access

Proteção de IoT

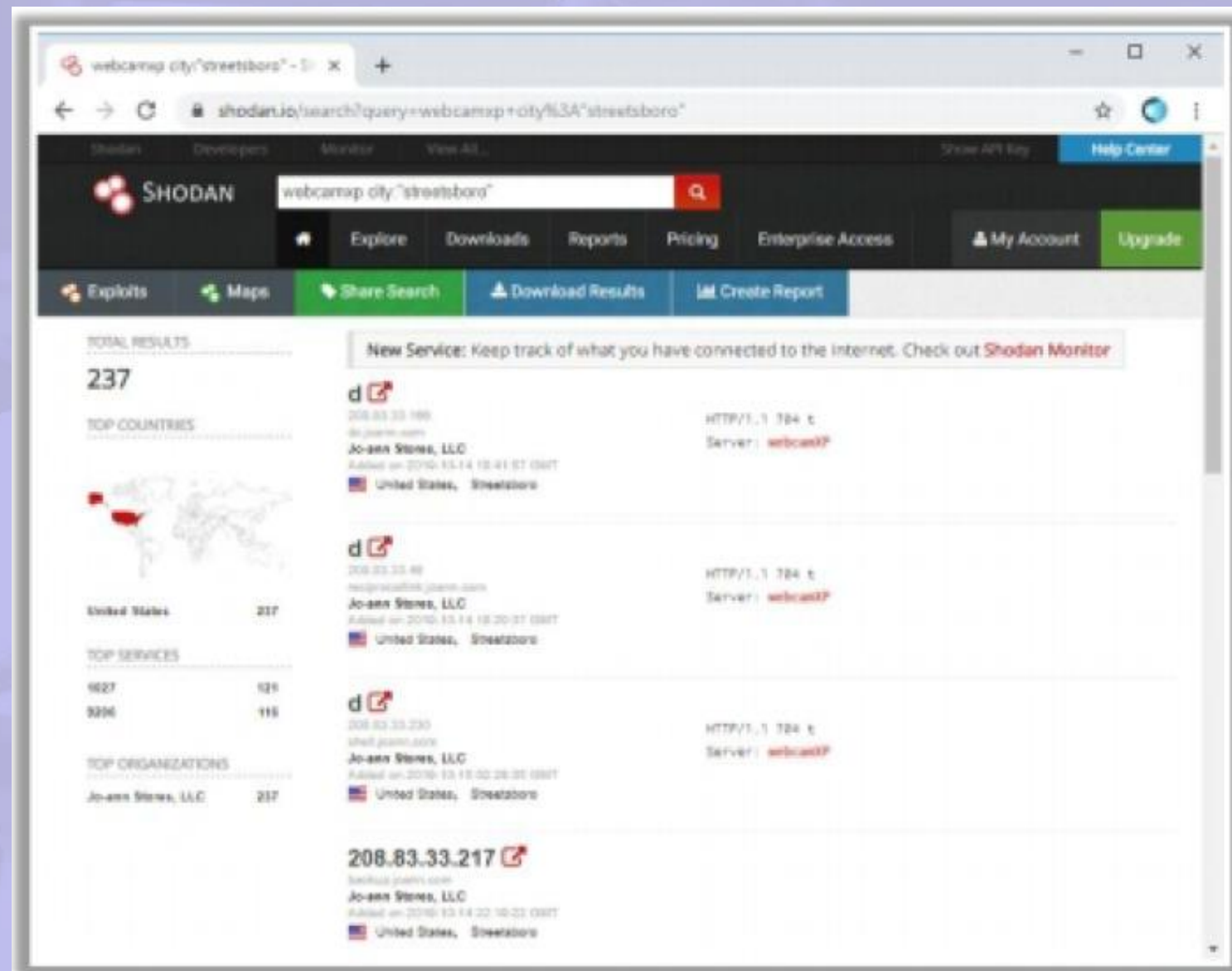
- Este scanner varre uma rede em busca de tipos específicos de dispositivos IoT para detectar se eles estão usando as credenciais padrão de fábrica.
- A intenção dessa ferramenta é ajudar as organizações a fazer a varredura de suas redes para detectar esses tipos de dispositivos IoT e identificar se as credenciais foram alteradas ou se o dispositivo ainda está usando a configuração de fábrica.

```
/Users/rapid7/freetools>perl iotScanner.pl 1.23.123.431,  
1.23.123.443,1.23.123.453,1.23.123.457,1.23.123.459,1.23.123.461,1.  
23.123.462,1.23.123.463,1.23.123.465,1.23.123.466,1.23.123.467,1.23.  
.123.469,1.23.123.472,1.23.123.473,1.23.123.475,1.23.123.477,1.23.1  
23.479,1.23.123.480,1.23.123.481  
[device 1.23.123.431 is of type Stardot still has default passwd  
device 1.23.123.443 is of type Arecont has changed passwd  
device 1.23.123.453 is of type American Dynamics has changed passwd  
device 1.23.123.457 is of type W-Box has changed passwd  
device 1.23.123.459 is of type Arecont has changed passwd  
device 1.23.123.461 is of type American Dynamics has changed passwd  
device 1.23.123.462 is of type W-Box has changed passwd  
device 1.23.123.463 is of type Arecont has changed passwd  
device 1.23.123.465 is of type American Dynamics has changed passwd  
device 1.23.123.466 is of type W-Box has changed passwd  
device 1.23.123.467 is of type Arecont has changed passwd  
device 1.23.123.469 is of type American Dynamics has changed passwd  
device 1.23.123.472 is of type W-Box has changed passwd  
device 1.23.123.473 is of type W-Box has changed passwd  
device 1.23.123.475 is of type W-Box has changed passwd  
device 1.23.123.477 is of type W-Box still has default passwd  
device 1.23.123.479 is of type Arecont has changed passwd  
device 1.23.123.480 is of type American Dynamics has changed passwd  
device 1.23.123.481 is of type American Dynamics has default passwd
```

Ferramentas de coleta de informações

Shodan

- O Shodan fornece informações sobre todos os dispositivos conectados à Internet, como roteadores, semáforos, câmeras CCTV, servidores e dispositivos domésticos inteligentes. Os invasores podem utilizar esta ferramenta para coletar informações como endereço IP, nome do host, ISP, localização do dispositivo e o banner do dispositivo IoT alvo. Os invasores podem coletar informações em um dispositivo alvo usando os filtros.



Ferramentas de coleta de informações

Censys

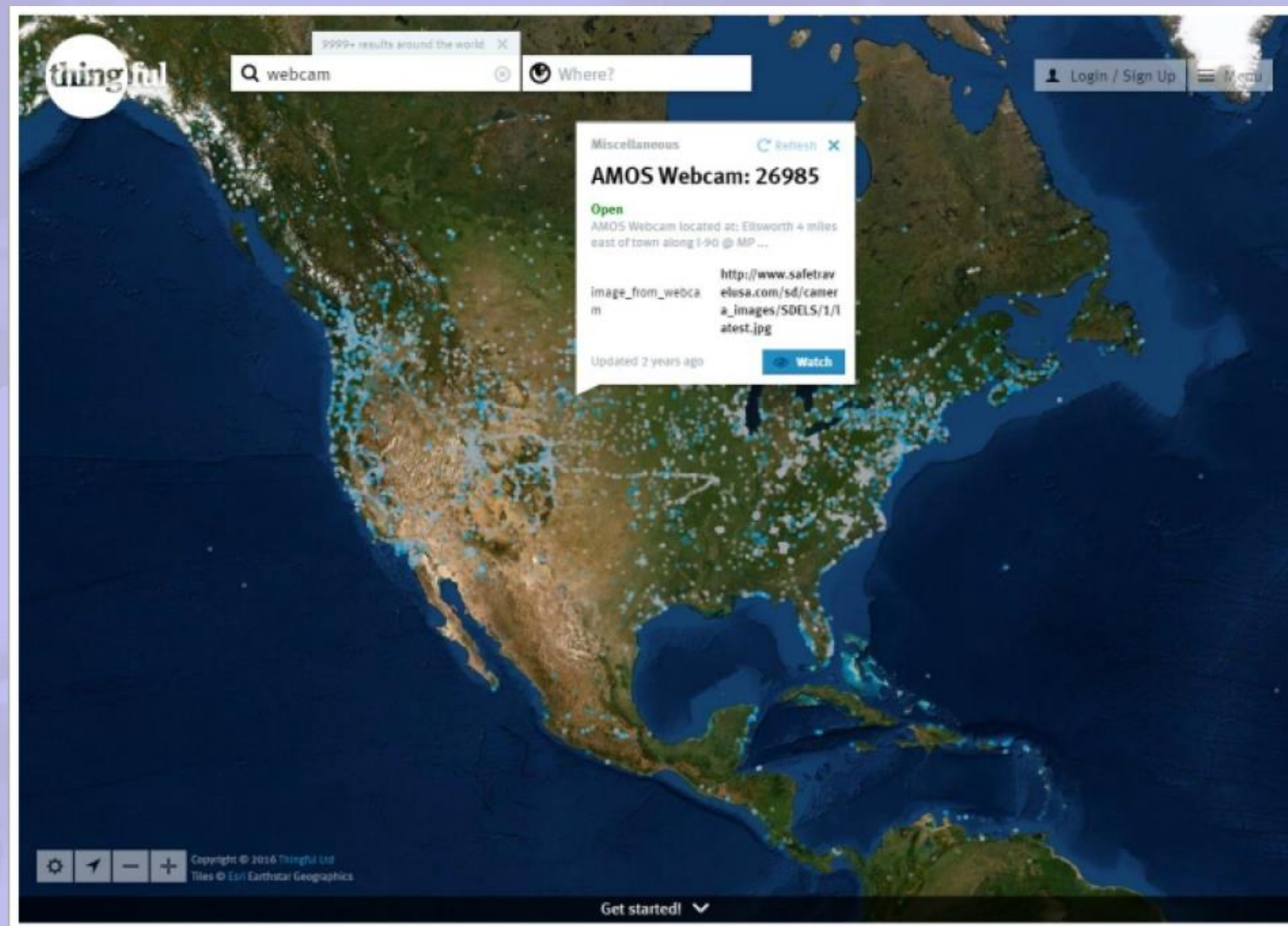
- Fonte: <https://censys.io>
- Censys é um mecanismo de busca público de fácil processamento de dados apoiado por dados coletados de varreduras contínuas em toda a Internet. Censys suporta pesquisas de texto completo em banners de protocolo e consulta uma ampla gama de campos derivados. Ele pode identificar dispositivos e redes vulneráveis específicos e gerar relatórios estatísticos sobre padrões e tendências de uso amplo.

The screenshot shows the Censys search interface. At the top, the Censys logo is on the left, and a search bar contains the query 'webcam'. Below the search bar, there are tabs for 'Results', 'Map', 'Metadata', 'Report', and 'Docs'. The 'Results' tab is selected. On the left side, there are two sections: 'Quick Filters' and 'Autonomous System:'. The 'Quick Filters' section has a link to 'Data Definitions'. The 'Autonomous System' section lists several ASes with their IP counts: 2,224 OVH, 2,099 COMCAST-7922 - Comcast Cable Communications, LLC, 1,662 MOJOHOST - MOJOHOST, 1,477 AMAZON-02 - Amazon.com, Inc., and 936 DIGITALOCEAN-ASN - DigitalOcean, LLC. Below this is a 'Protocol:' section with counts for various protocols: 38.67K 80/http, 18.69K 443/https, 8,594 21/ftp, 8,013 22/ssh, and 6,291 110/pop3. There is also a 'Tag:' section with counts for various tags: 41.89K http, 17.93K https, 8,594 ftp, 8,013 ssh, and 7,758 smtp. The main content area on the right is titled 'IPv4 Hosts' and shows a list of results. The first result is '159.69.123.235 (mars.foto-webcam.eu)' with details about the host, including its IP address, location (Germany), and the services it provides (SSH, HTTPS, HTTP). The second result is '213.133.127.197 (cdn.foto-webcam.eu)' with similar details. The third result is '194.230.47.202 (livecam.zermatt.net)' with details about the host, including its IP address, location (Switzerland), and the services it provides (FTP, HTTP). The fourth result is '78.47.202.110 (guffert.foto-webcam.eu)' with details about the host, including its IP address, location (Germany), and the services it provides (SSH, HTTPS, HTTP). The fifth result is '88.198.51.143 (static.88-198-51-143.clients.your-server.de)' with details about the host, including its IP address, location (Germany), and the services it provides (FTP, HTTPS, HTTP).

Ferramentas de coleta de informações

Thingful

- Thingful é um mecanismo de busca para encontrar e usar dados abertos de IoT de todo o mundo. Isto ajuda as organizações a tomar melhores decisões com dados de IoT externos. Ele coleta dados de IoT em tempo real em dezenas de setores, incluindo clima, meio ambiente, cidades inteligentes, energia e transporte. Os canais de dados do Thingful tornam rápido e fácil encontrar e usar os dados IoT.
- <http://www.thingful.net>




Ferramentas de sniffer IoT

Os administradores de sistema usam ferramentas automatizadas para monitorar sua rede e os dispositivos conectados à rede, mas os invasores usam essas ferramentas de forma inadequada para “snifar” os dados da rede.

- Suphacap <https://www.suphammer.net>
- CloudShark (<https://cloudshark.io>)
- Ubiqua Protocol Analyzer (<https://www.ubiogix.com>)
- Perytons Protocol Analyzers (<http://www.perytons.com>)
- tcpdump (<https://www.tcpdump.org>)
- Open Sniffer (<https://www.sewio.net>)


Sniffing Tools




Suphacap, a Z-Wave sniffer, is used to **sniff the traffic**, perform **real-time monitoring**, and **capture packets** from all Z-Wave networks

```
Suphacap — 80x24 — 115200.8.N.1
[03F949EC] 01 -> 34 : Class 37, Method 02
[03F949EC] 34 -> 01 :
[03F949EC] 34 -> 01 : Class 37, Method 03, Param @x00
[03F949EC] 01 -> 34 :
[03F949EC] 01 -> 05 : Class 96, Method 06, Param @x06022502
[03F949EC] 01 -> 05 : Class 96, Method 06, Param @x06022502
[03F949EC] 01 -> 05 : Class 96, Method 06, Param @x06022502
[03F949EC] 01 -> 05 :
[03F949EC] 01 -> 34 : Class 37, Method 02
Suphacap v1.0.1 - (C) Jon Suphammer
Commands:
h[homeid]
n[nodeid]
c[class]
r<reg>=ch>
q<@>|> - raw
i<@>|> - invalid crc
o<@>|> - rssi
X - exit
c49
[03F949EC] 01 -> 39 : Class 49, Method 04, Param @x04
[03F949EC] 39 -> 01 : Class 49, Method 05, Param @x0504220000
```


<https://www.suphammer.net>




CloudShark
<https://cloudshark.io>




Ubiqua Protocol Analyzer
<https://www.ubiogix.com>



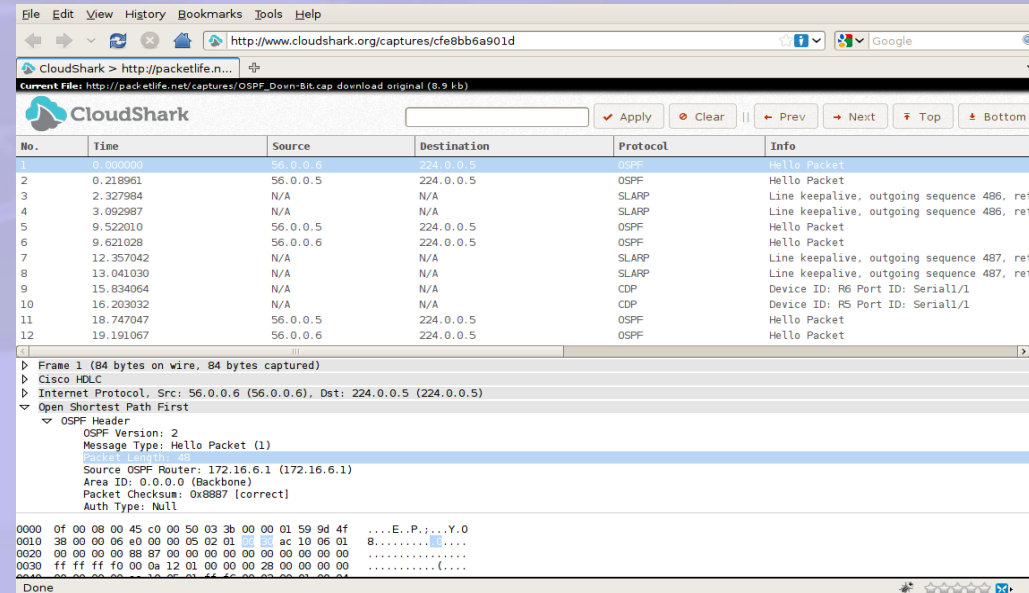
Perytons Protocol Analyzers
<http://www.perytons.com>



Tcpdump
<https://www.tcpdump.org>



Open Sniffer
<https://www.sewio.net>



The screenshot shows the CloudShark web interface with a packet capture of an OSPF Hello packet. The table below represents the data shown in the 'Info' column of the packet list.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	56.0.0.6	224.0.0.5	OSPF	Hello Packet
2	0.218961	56.0.0.5	224.0.0.5	OSPF	Hello Packet
3	2.327984	N/A	N/A	SLARP	Line keepalive, outgoing sequence 486, ret
4	3.092987	N/A	N/A	SLARP	Line keepalive, outgoing sequence 486, ret
5	9.522010	56.0.0.5	224.0.0.5	OSPF	Hello Packet
6	9.621028	56.0.0.6	224.0.0.5	OSPF	Hello Packet
7	12.357042	N/A	N/A	SLARP	Line keepalive, outgoing sequence 487, ret
8	13.041030	N/A	N/A	SLARP	Line keepalive, outgoing sequence 487, ret
9	15.834064	N/A	N/A	CDP	Device ID: R6 Port ID: Serial1/1
10	16.203032	N/A	N/A	CDP	Device ID: R5 Port ID: Serial1/1
11	18.747047	56.0.0.5	224.0.0.5	OSPF	Hello Packet
12	19.191067	56.0.0.6	224.0.0.5	OSPF	Hello Packet

The detailed view of the selected packet (Frame 1) shows:

- Frame 1 (84 bytes on wire, 84 bytes captured)
- Cisco HDLC
- Internet Protocol, Src: 56.0.0.6 (56.0.0.6), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
- OSPF Header
- OSPF Version: 2
- Message Type: Hello Packet (1)
- Source OSPF Router: 172.16.6.1 (172.16.6.1)
- Area ID: 0.0.0.0 (Backbone)
- Packet Checksum: 0x8887 [correct]
- Auth Type: Null

The hex dump at the bottom shows the raw packet data in hexadecimal and ASCII format.

Ferramentas de hacking IoT

Listadas abaixo estão algumas das ferramentas de hacking de IoT utilizadas por invasores para explorar dispositivos e redes de IoT alvo para realizar vários ataques, como DDoS, jamming e ataques BlueBorne.

- Firmalyzer Enterprise <https://firmalyzer.com>
- Firmwalker (<https://github.com>)
- rfcatt-rolljam (<https://github.com>)
- KillerBee (<https://github.com>)
- GATTack.io (<http://www.gattack.io>)
- JTAGULATOR® (<http://www.grandideastudio.com>)



Firmwalker
<https://github.com>



rfcatt-rolljam
<https://github.com>



KillerBee
<https://github.com>



GATTack.io
<http://www.gattack.io>



JTAGULATOR®
<http://www.grandideastudio.com>

Como se defender contra hackers de IoT

IoT Framework Security Considerations

1

EDGE

- Communications encryption
- Storage encryption
- Update components
- No default passwords

2

GATEWAY

- Multi-directional encrypted communications
- Strong authentication of all the components
- Automatic updates

3

CLOUD PLATFORM

- Encrypted communications
- Secure web interface
- Authentication
- Encrypted storage
- Automatic updates


4

MOBILE

- Local storage security
- Encrypted communications channels
- Multi-factor authentication
- Account lockout mechanism

Gerenciamento de dispositivos IoT

- O gerenciamento de dispositivos IoT ajuda os profissionais de segurança a rastrear, monitorar e gerenciar dispositivos IoT físicos de um local remoto. podem usar soluções como Azure IoT Central, Oracle IoT Asset Monitoring Cloud e Predix para executar o gerenciamento de dispositivos IoT. Essas soluções permitem que atualizemos o firmware remotamente. Além disso, o gerenciamento de dispositivos IoT ajuda a fornecer permissões e melhorar os recursos de segurança para garantir a proteção contra várias vulnerabilidades.



The screenshot displays the Azure IoT Central interface. On the left, a sidebar lists navigation options like 'Create a resource', 'Dashboard', and 'All services'. The main area is titled 'Azure IoT Central' and shows an 'Overview' page. It features several key metrics: 'Threat prevention' with a 'Device recommendations' gauge showing 57 items, 'Health monitoring' with a 'T index' bar chart, and 'Threat detection' with 'Device security alerts' and 'Resource security alerts' bar charts. A 'Most attached devices' section shows 2852 devices. The bottom right corner of the screenshot includes the URL <https://azure.microsoft.com>.

IoT device management helps in supporting IoT solutions by using any software tools and processes and helps in **onboarding latest devices** securely and promptly

It allows the users to track, monitor, and manage physical IoT devices and forces users to remotely **update the firmware**

IoT device management helps in providing permissions and security capabilities for protection against vulnerabilities

IoT Device Management Solutions

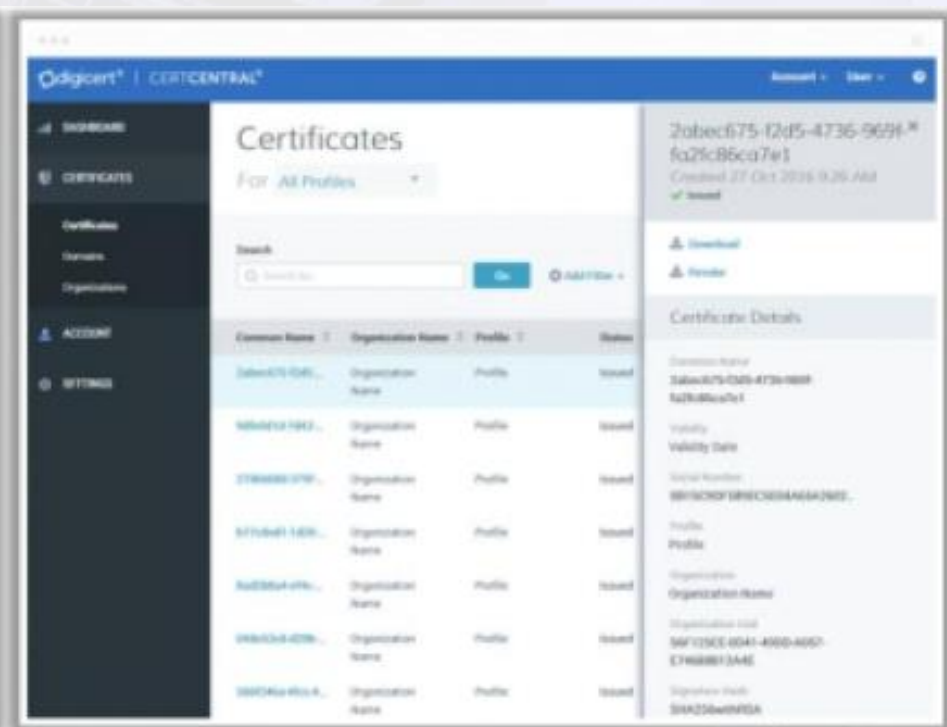
- Oracle IoT Asset Monitoring Cloud (<https://www.oracle.com>)
- Predix (<https://www.ge.com>)
- Cloud IoT Core (<https://cloud.google.com>)
- IBM Watson IoT Platform (<https://www.ibm.com>)
- AT&T IoT Platform (<https://iotplatform.att.com>)

Ferramentas de segurança IoT

Para compreender e analisar vários fatores de risco, soluções de segurança adequadas devem ser incorporadas para proteger os dispositivos IoT. O uso de ferramentas de segurança IoT ajuda as organizações a limitar significativamente as vulnerabilidades de segurança, protegendo assim os dispositivos e redes IoT de diferentes tipos de ataques.


















<https://www.teskalabs.com>



<https://www.digicert.com>

Ferramentas de segurança IoT

 FortiNAC https://www.fortinet.com	 Cisco IoT Threat Defense https://www.cisco.com	 Norton Core https://us.norton.com
 Pulse: IoT Security Platform https://www.pwnieexpress.com	 AWS IoT Device Defender https://aws.amazon.com	 zvelo IoT Security Solution https://zvelo.com
 Symantec IoT Security https://www.symantec.com	 Bayshore Industrial Cyber Protection Platform https://www.bayshorenetworks.com	 Barbara https://barbaraiot.com
 darktarce https://www.darktrace.com	 Endpoint Protection Suite https://www.securetrust.com	 Sternum https://www.sternumiot.com
 Symantec Critical System Protection https://www.symantec.com	 NSFOCUS ADS https://nsfocusglobal.com	 Bullguard IoT Scanner https://iots Scanner.bullguard.com/

Conceitos sobre OT:

A tecnologia operacional (OT) desempenha um papel importante na sociedade moderna de hoje, pois impulsiona uma coleção de dispositivos projetados para trabalharem juntos como um sistema integrado ou homogêneo.

OT é uma combinação de hardware e software usado para monitorar, executar e controlar ativos de processos industriais. Antes de aprender como hackear OT, é importante entender seus conceitos básicos.



CEHv12

18.IoT & OT Hacking



O que é o OT

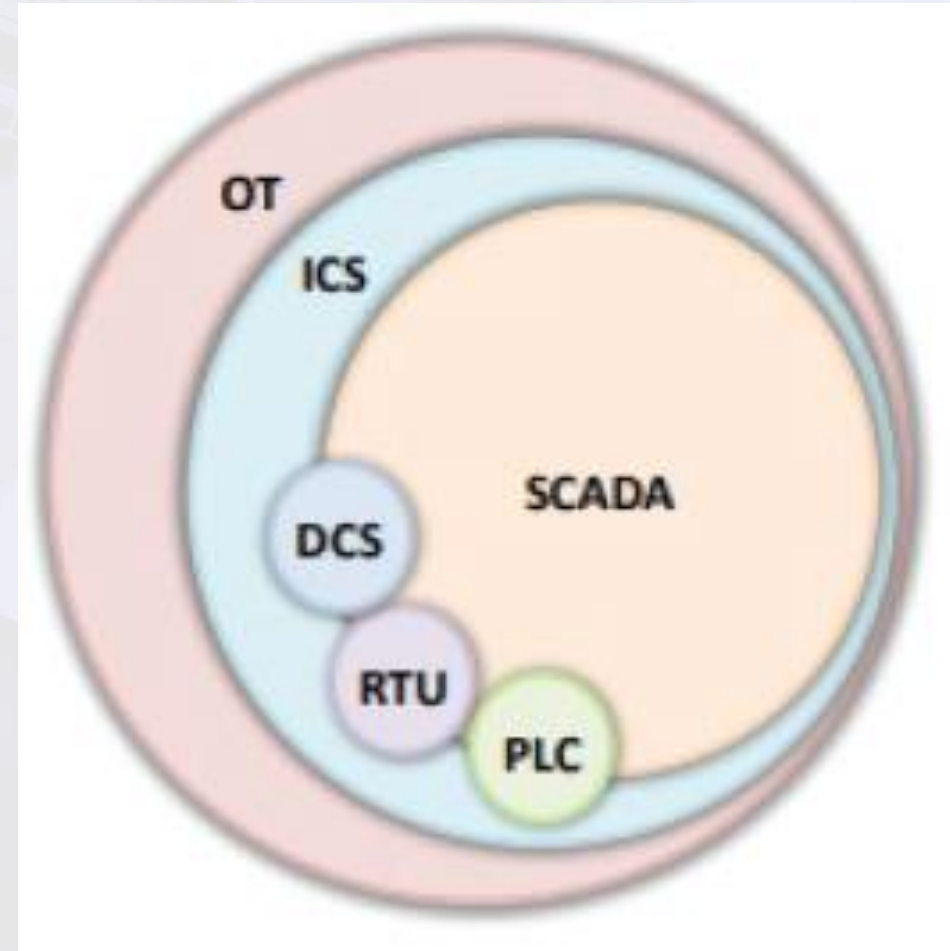
OT é uma combinação de software e hardware projetado para detectar ou causar mudanças nas operações industriais por meio do monitoramento direto e/ou controle de dispositivos físicos industriais.

Esses dispositivos incluem interruptores, bombas, luzes, sensores, câmeras de vigilância, elevadores, robôs, válvulas e sistemas de resfriamento e aquecimento. Qualquer sistema que analise e processe dados operacionais (como componentes técnicos, eletrônicos, telecomunicações e sistemas de computador) pode fazer parte da OT.

Componentes do OT

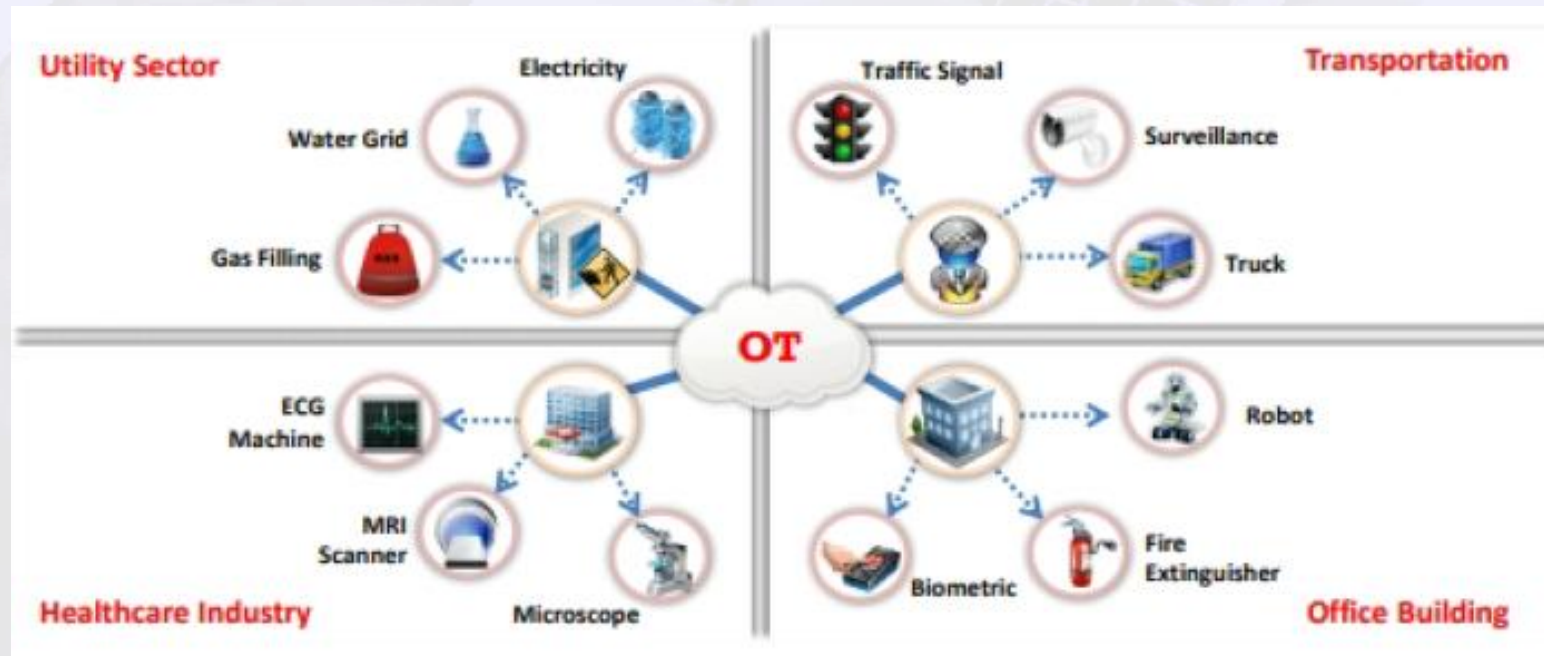
Esta tecnologia consiste em:

Sistemas de Controle Industrial (ICSs), que incluem Controle Supervisório e Aquisição de Dados (SCADA), Unidades Terminais Remotas (RTU), Controladores Lógicos Programáveis (PLC), Sistemas de Controle Distribuído (DCSs) e muitos outros sistemas de rede dedicados que auxiliam no monitoramento e controle de operações industriais.



Onde encontramos o OT

Os sistemas OT são utilizados nos setores de manufatura, mineração, saúde, construção, transporte, petróleo e gás, defesa e serviços públicos, bem como muitos outros setores, para garantir a segurança de dispositivos físicos e suas operações em redes.



Desafios do OT

Os sistemas OT empregam abordagens diferentes para projetar hardware e protocolos que não estão familiarizados com a TI. O suporte a versões mais antigas de software e hardware tornam os sistemas OT mais vulneráveis a ataques cibernéticos, pois o desenvolvimento de correções ou patches para eles é muito difícil.



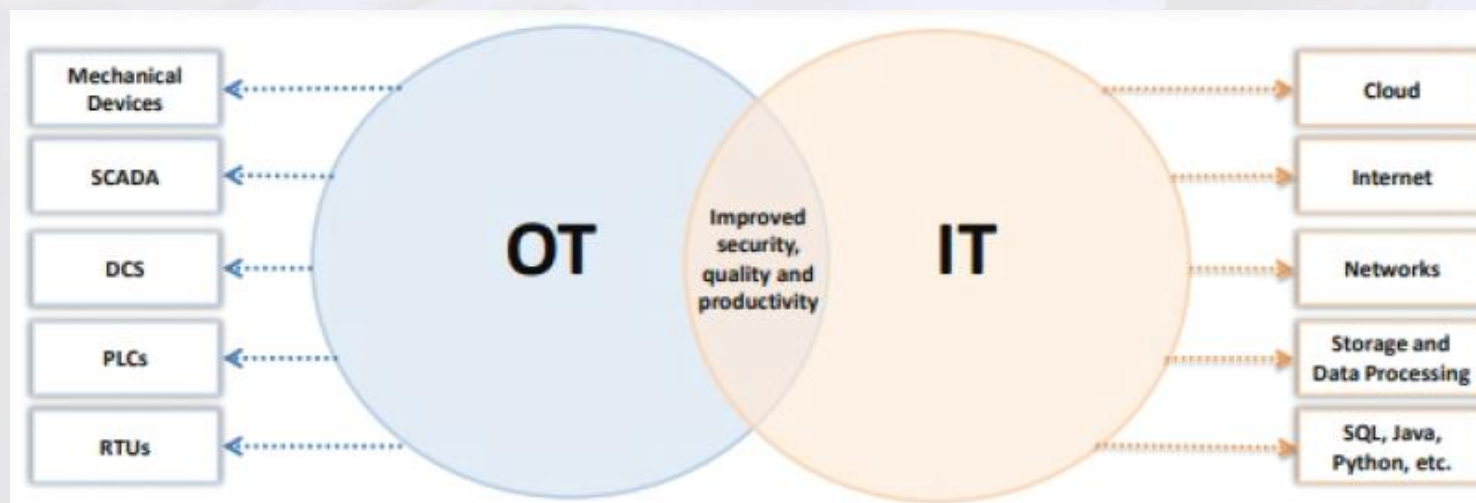
Terminologia Essencial

Essential Terminology

Assets	OT systems consist of physical assets such as sensors and actuators, servers, workstations, network devices, and PLCs, and logical assets such as flow graphics, program logic, databases, firmware, and firewall rules
Zones and Conduits	A network segregation technique used to isolate the networks and assets to impose and maintain strong access control mechanisms
Industrial Network	A network of automated control systems is known as an industrial network
Business Network	It comprises of a network of systems that offer information infrastructure to the business
Industrial Protocols	Protocols used for serial communication and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.
Network Perimeter	It is the outermost boundary of a network zone i.e. closed group of assets
Electronic Security Perimeter	It is referred to as the boundary between secure and insecure zones
Critical Infrastructure	A collection of physical or logical systems and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health

Convergência IT/OT

É a integração de sistemas de computação de TI (tecnologia da informação) e sistemas de monitoramento de operação de OT. Preencher a lacuna entre TI e OT pode melhorar o negócio como um todo, produzindo resultados mais rápidos e eficientes. A convergência não envolve apenas a combinação de tecnologias, mas também equipes e operações. As equipes de TI e OT são tradicionalmente separadas e localizadas em seus respectivos domínios.



Integração Modelo PURDUE

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process



Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.