

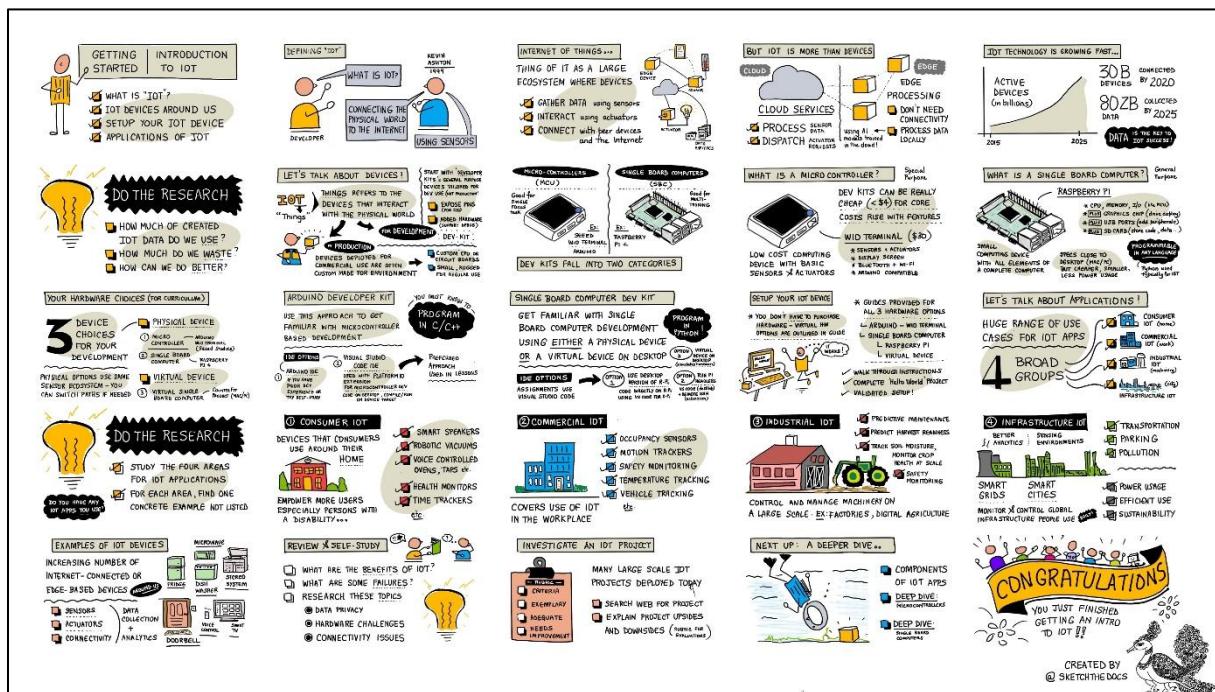
## Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego IoT - Laboratorium 12 – IoT Security Part 1

Forma: praca w samodzielna / małe zespoły (2 - 4 osoby)

### IoT

- <https://github.com/microsoft/IoT-For-Beginners>
- <https://github.com/V33RU/awesome-connected-things-sec>

Internet rzeczy (IoT) odnosi się do sieci urządzeń fizycznych, które łączą się i wymieniają dane między sobą oraz systemami opartymi na chmurze za pośrednictwem Internetu. Prawdopodobnie codziennie używasz takich urządzeń. Niektóre przykłady urządzeń IoT obejmują urządzenia inteligentnego domu, urządzenia do noszenia na sobie i osobiste urządzenia medyczne. Podatne na zagrożenia i niezabezpieczone urządzenia IoT są narażone na ryzyko zhakowania i ujawnienia poufnych informacji ofiary cyberprzestępcom, którzy następnie mogą wykorzystać te informacje do złośliwych działań lub uzyskania korzyści finansowych.



**Materiały dodatkowe:**

- <https://www.youtube.com/watch?v=YPcOwKtRuDQ>
- <https://github.com/OWASP/owasp-istg>
- <https://scriptingxss.gitbook.io/firmware-security-testing-methodology/>
- <https://academy.tcm-sec.com/p/beginner-s-guide-to-iot-and-hardware-hacking>
- <https://www.hackthebox.com/machines/mirai>
- [https://www.youtube.com/watch?v=mN7tHGBbg\\_Y](https://www.youtube.com/watch?v=mN7tHGBbg_Y)
- <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>
- <https://iotsecurityfoundation.org/>
- <https://github.com/V33RU/awesome-connected-things-sec>
- <https://github.com/attify/firmware-analysis-toolkit>
- <https://github.com/firmadyne/firmadyne>
- <https://github.com/microsoft/IoT-For-Beginners>
- <https://github.com/riot-os/riot-course>
- <https://riot-os.github.io/riot-course/slides/06-security-with-riot/#1>

## Zadania praktyczne

### Zadanie 1 – Instalacja i pentest OWASP IoTGoat

- <https://github.com/OWASP/IoTGoat>
  - [https://www.youtube.com/watch?v=mN7tHGBbg\\_Y](https://www.youtube.com/watch?v=mN7tHGBbg_Y)
  - <https://williamzujkowski.github.io/posts/iot-security-in-your-home-lab-lessons-from-owasp-iotgoat/>

Zadania do wykonania:

- <https://github.com/OWASP/IoTGoat/wiki/IoTGoat-challenges>
  - Rozwiązania zadań: <https://github.com/OWASP/IoTGoat/wiki/Challenge-solutions>

Różne metody instalacji:

- <https://github.com/OWASP/IoTGoat/wiki/Getting-started#how-to-get-started>

Ewentualnie instalacja z wykorzystaniem docker (lepiej wykorzystać metodę z maszyną wirtualną 😊):

```
#!/bin/bash
# IoT Security Lab Setup Script
# Combines tools installation, IoTGoat deployment, and firmware analysis toolkit

# Core analysis tools installation
echo "[*] Installing core IoT analysis tools..."
sudo apt-get update
sudo apt-get install -y \
    wireshark \
    nmap \
    binwalk \
    firmware-mod-kit \
    mosquitto-clients \
    john \
    hashcat

# Python tools for IoT testing
pip install paho-mqtt scapy pycryptodome

# IoTGoat Docker deployment
echo "[*] Deploying OWASP IoTGoat..."
git clone https://github.com/OWASP/IoTGoat.git
cd IoTGoat/docker

# Build the Docker container (isolated environment)
docker build -t iotgoat .
docker compose up --build

# Firmware analysis toolkit
echo "[*] Firmware analysis commands:"
echo "binwalk -e iotgoat_firmware.bin"
echo "grep -r 'password|passwd|pwd|api_key|secret' _iotgoat_firmware.bin.extracted/"
echo "unsquashfs -d extracted_fs _iotgoat_firmware.bin.extracted/*.*squashfs"
echo "checksec --file=extracted_fs/usr/bin/iot_service"
```

Po ukończeniu build:

```
ssh -o HostKeyAlgorithms=+ssh=rsa iotgoatuser@localhost -p 2222
```

Dodatkowo należy pobrać plik **IoTGoat-raspberry-pi2.img**: <https://github.com/OWASP/IoTGoat/releases/tag/v1.0>