PT REPORT

CySDR

EXECUTIVE SUMMARY:

Objective: The primary goal of this penetration test was to evaluate the security posture of IoT devices within the "CySDR" simulation, a web-based platform developed by RadioElectic to raise awareness about smart city security. The focus was on exploiting vulnerabilities in an IP camera and an automated car system using Software Defined Radio (SDR) techniques.

CONCLUSIONS:

In my humble opinion, using the simulator is fun, experiential and educational. Send me to research about the frequency of things on the internet. These activities not only highlight the versatility of SDR in manipulating IoT devices but also underscore the need for robust security protocols in smart city infrastructures.

But the IoT expert conducted on the CySDR simulation developed by RadioElectric has provided valuable insights into the security vulnerabilities present in smart city IoT devices. The exercise successfully demonstrated two critical vulnerabilities: one in an IP camera operating at 2.42 GHz and another in a car's access control system at 432 MHz. These findings highlight a significant concern in the realm of IoT security, particularly in the context of smart cities where such devices are increasingly prevalent.

In relation to the IP camera critical (9.8) risk lifting according to CVSS Calculator v 3.1, and the car access control also critical (9.4) by the same Calculator.

PT REPORT

CONCLUSION:

Description:

The web-based simulation developed for RadioElectric's smart city security awareness campaign successfully demonstrates the intricate interplay between Internet of Things (IoT) devices and Software-Defined Radio (SDR) technology. By engaging users in a hands-on, interactive environment, the simulation effectively raises awareness about the security implications .inherent in smart city ecosystems

Details:

Key features of the simulation include the ability for users to control a character and an SDR device using simple keyboard commands. The simulation challenges users to utilize specific radio frequencies to bypass security mechanisms of different IoT devices. These activities not only highlight the versatility of SDR in manipulating IoT devices but also underscore the need for robust security protocols in smart city infrastructures.

The exploitation of the car's IP camera and access control system highlighted the ease with which malicious actors can intercept and manipulate unsecured wireless communications. This test, conducted in a simulated environment, reflects real-world scenarios where attackers can gain unauthorized access to critical infrastructure and private spaces. The discovered vulnerabilities, if not addressed in actual smart city implementations, could lead to serious privacy violations.

This penetration test highlights the urgent need for manufacturers and city planners to prioritize the security of IoT devices. Implementing strong security measures such as encrypted communication, frequency hopping, rolling codes and advanced encryption methods is imperative. Additionally, ongoing security assessments and updates are essential to protect against threats.

In my conclusion, the CySDR simulation serves as a crucial reminder of the risks involved in the growing adoption of IoT technologies in smart cities. It is imperative for stakeholders to recognize these vulnerabilities and take proactive steps to strengthen the security of these systems.

Evidence:

To make this simulation I need to search information that can help to bypass the way to end.

Its first start whit way to find in which frequency I need to use to pass the IP camera.

After a research in the internet I find the frequency to IP camera is 2.42GHZ.

FIGURE 1: IP camera

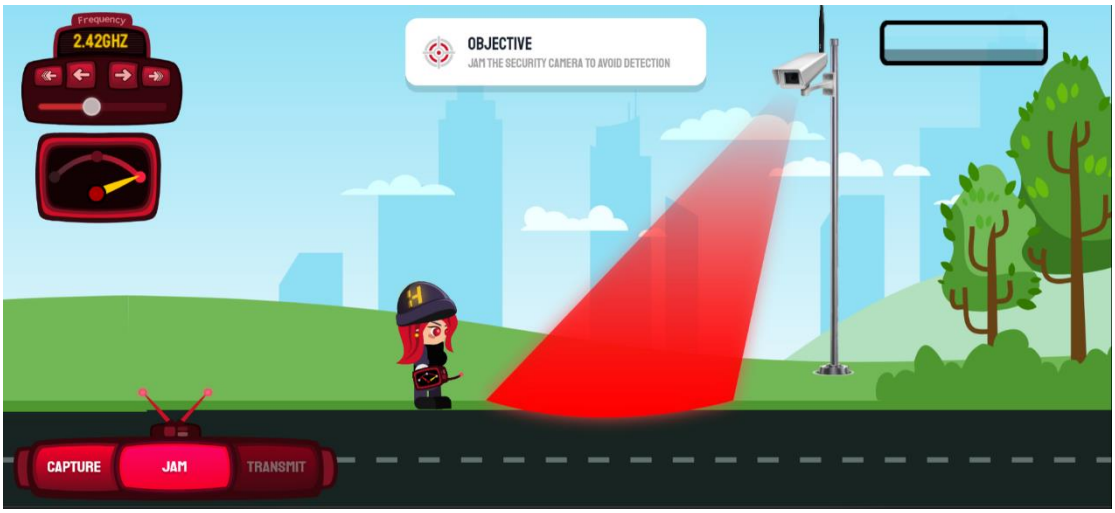
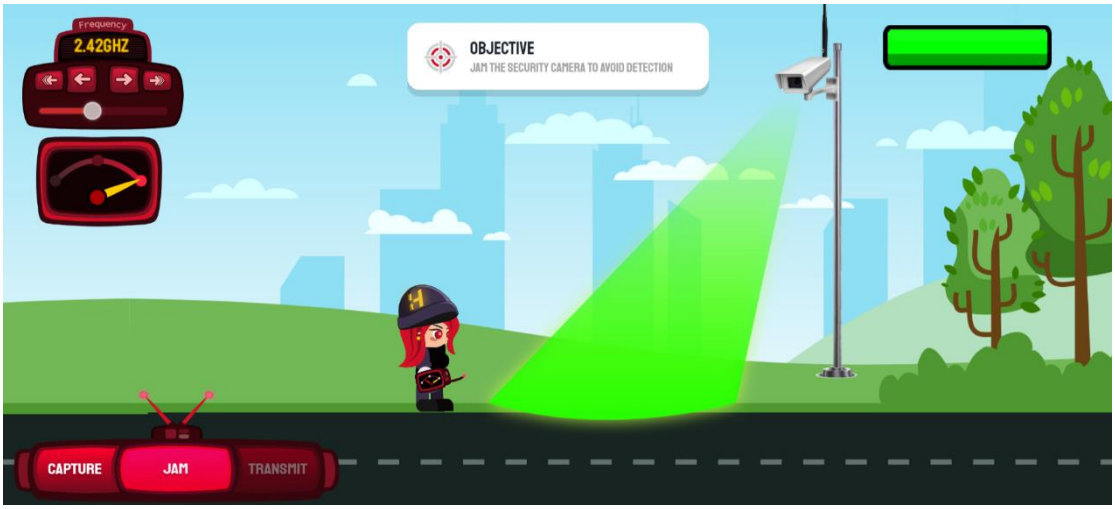


FIGURE 2:Bypass the IP camere



After that I need to capture the key car whit my SDR and transmit it to get access to the car.

I research in the internet then I find a few options that use in U.S.A and in Europe. In the end I find that in this simulation use like in Europe that need a 433MHZ to capture the signal for car key.

FIGURE 3: get whit my SDR the car key fruquncy

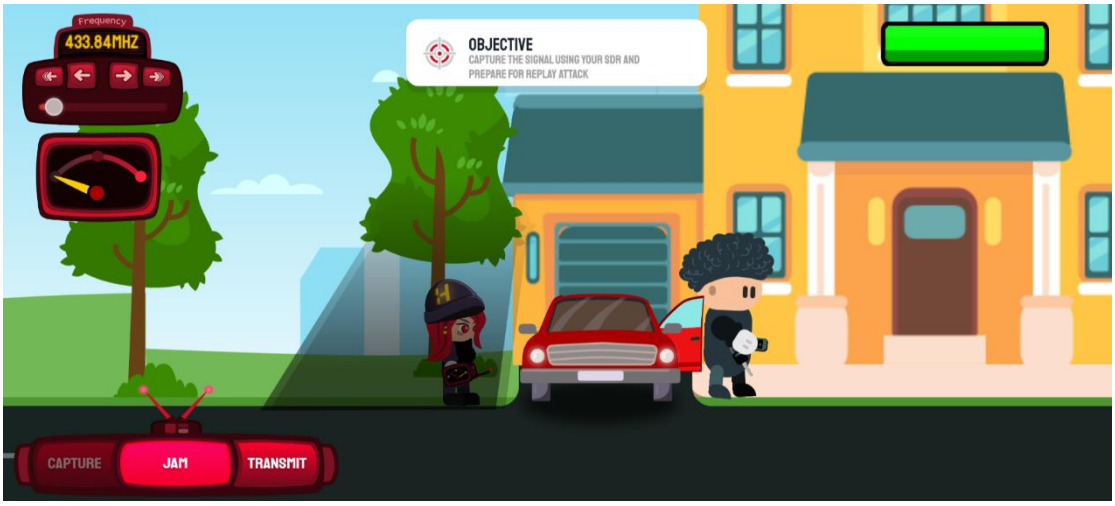
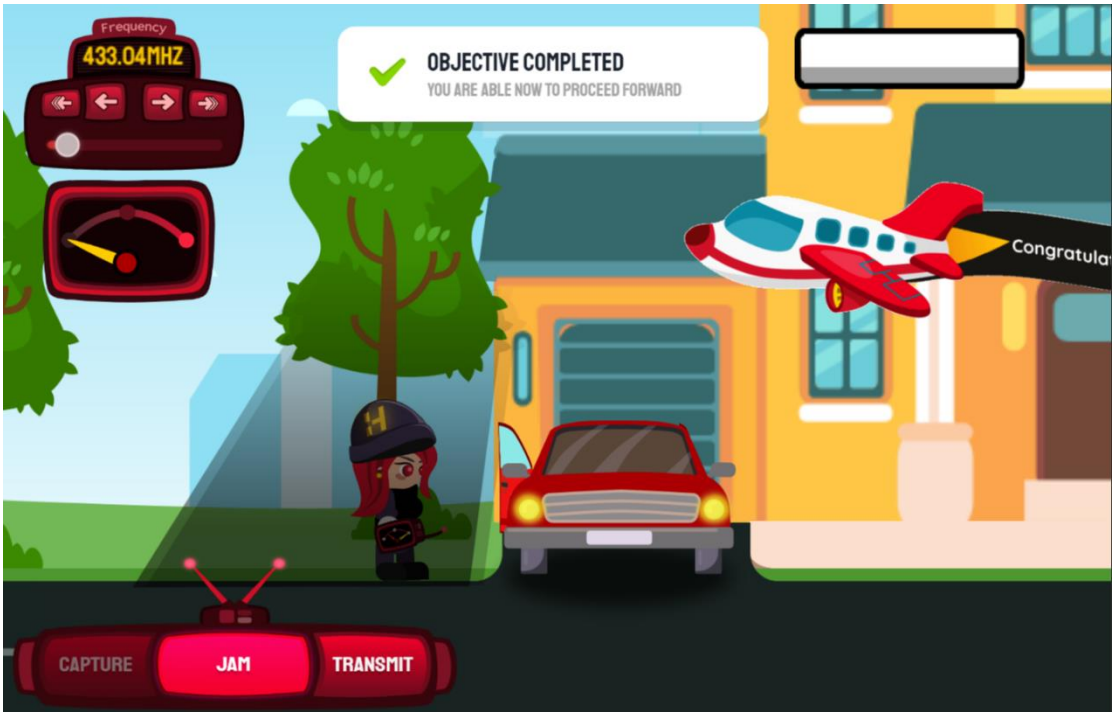


FIGURE 4: transmit the frequncy of the key car on the car.



Recommend suggestions:

First of all I am very happy about the desire to increase awareness of illegal activities that can unfortunately exist in a smart city.

Secend as I said earlier to prioritize the security of IOT devices in smart cities, and increase awareness of the danger in them even for the older generation that is less likely to connect to the use of simulation.