# Huston we have a hack!

Vatafu Vladut
Timisoara, Romania

## Overview

This ctf aims to simulate a process for testing a LoRA / LPWAN network.

The scenario is as follows: “You, a hacker, received an anonymous tip as if it were an intelligence agency launched a contest like CICADA 3301 and those who end up finishing all their problems are automatically recruited. Your ultimate goal is to have total control over the network, so that data exfiltration, monitoring, locating and executing unauthorized code can be possible.”

## Specifications

The proposed tasks range from web security to reverse engineering procedures, network security, cryptographic attacks. The first test will consist in testing a web page that once compromised will allow taking control over the gateway server(a simple sqli). This server symbolizes the "door" or access to the base station (SATcom) known as the "gateway" that communicates with the "satellite".The second problem is part of the network security category, more precisely of the post exploitation category, because once the server access is obtained, you must obtain access in the internal network in order to have access to the rest of the ctf. The "attacker" must demonstrate minimal knowledge using a technique called network pivotation by performing the port relay procedure to bypass firewall restrictions. Once in the internal network, the player can choose from a variety of issues, such as:

- Analysis of a firmware running on an android, the firmware being subsequently modified, it being trojaned and having a hidden function in the GSM stack (AT commands firmware) that allows the execution of code on an unauthorized device by sending a special SMS.

-Decryption of data received from an iGATE (ARPS gateway) for the data exfiltration category, these being encrypted with the RSA and ECC algorithm (y ^ 2 = x ^ 3 + ax + b over GF (p) ). Although this data is encrypted because those who implemented the algorithms did not implement it well this data set is vulnerable to the following attacks: rabin attack when e = 1 and baby step giant step dlp

-Interception and decryption of the rf signal transmitted by us containing a picture with the flag for the task

-ESP32 OTA unlock crate cryptographic vulnerability encryption in AES OFB iv encryption, by xor iv and cipher -> flag which requires physical presence at the crate , the geolocation for the create will be taken from the task with the iGate system

-"Spacial"(reverse connection using a special packer to the other dreamcatcher) pivot so I switch to another network and I have a PC that I have to hack that keeps a bitcoin address vulnerable to invalid curve attack

-Something with md5 collision / length extension attack

-Proposals

## Hawrdware prices

### I. Dreamcatchers

100 $

### II. Usrb b210

£1,270.00 GBP without the necessary antennas with antennas overall price $ 1500

## Issues

-We want to give prizes

-How do we make it accessible from the outside or do we just want it for RO