October 2022

D

ECSC 2021 – Prague

**Challenge author:** [Patrik Vácal](https://www.linkedin.com/mwlite/in/patrikvacal)

Writeup for challenge Brainy Weights

ABOUT ECSC

The growing need for IT security professionals is widely acknowledged worldwide. To help mitigate this shortage of skills, many countries launched national cybersecurity competitions targeting towards students, university graduates or even non-ICT professionals with a clear aim to find new and young cyber talents and encourage young people to pursue a career in cyber security. The European Cyber Security Challenge (ECSC) leverages on these competitions by adding a pan-European layer.

The European Cyber Security Challenge is an initiative by the European Union Agency for Cybersecurity (ENISA) and aims at enhancing cybersecurity talent across Europe and connecting high potentials with industry leading organizations.

CONTACT

For contacting the authors, please use ecsc@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Authors/acknowledgements

Patrik Vácal, ECSC 2021 Organization Team
Jiří Bartušek, ECSC 2021 Organization Team – this document’s author

legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

copyright notice

© European Union Agency for Cybersecurity (ENISA), 2022
Reproduction is authorised provided the source is acknowledged.

Table of contents

[1. Information regarding the challenge 3](#_Toc121692234)

[1.1 Description of the challenge 3](#_Toc121692235)

[1.2 Challenge specification 3](#_Toc121692236)

[1.3 Technical Specification 3](#_Toc121692237)

[1.3.1 Required infrastructure 3](#_Toc121692238)

[1.3.2 Provided files 3](#_Toc121692239)

[2. Attack Scenario 4](#_Toc121692240)

[2.1 Description of the scenario 4](#_Toc121692241)

[2.2 Installation Instructions 4](#_Toc121692242)

[2.3 Tools needed for solving the challenge 4](#_Toc121692243)

[2.4 Walkthrough (Writeup) 4](#_Toc121692244)

1. Information regarding the challenge

## Description of the challenge

This AI spent too much time on this task.

## Challenge specification

* Challenge Category: Artificial Intelligence
* Difficulty: Medium
* Expected time to solve: 1h

## Technical Specification

The challenge is made up of 2 files – Tensorflow H5 Keras model and plaintext file containing flag, that contestant needs to finish the challenge.

The challenge is static: **all files are provided to contesters for analysis**.

### Required infrastructure

No infrastructure is required to prepare the challenge. Solving can be done offline. More in *2.2 Installation Instructions*.

### Provided files

Figure 1: List of files

|  |  |  |  |
| --- | --- | --- | --- |
| File name | Format | Comment | Checksum (SHA256) |
| BrainyWeights.h5 | H5 Keras Model | Challenge file | d1ff456fe8a765432940e78fac19eadee7c15c3f63ef04288a3ceb24a3ab9f96 |
| flag.txt | Text File | Challenge file | 8bc47f8e8e85c50973714b16592437be2a4514ce8d15fb4c3d6df3ce232de792 |

1. Attack Scenario

## Description of the scenario

Participants needs to find a key inside the Tensorflow model. By finding that key, you can use AES ECB decipher tool to get the flag.

## Installation Instructions

You have to distribute both files to the contestants.

## Tools needed for solving the challenge

Needed tools are:

* General Linux tools
* Scripting language

## Walkthrough (Writeup)

By simple Google search, you can find out what h5 does – it is a Keras H5 Tensorflow model. For faster analysis, you can load this file directly into Tensorflow. By doing that, you can find out that the output of the model has 256 elements – all of them are between 0 and 1.

You can input practically anything into the model as input for being able to predict the key – for example zeros. The model will show you results where you can take the mean of each element that you can round to integers and convert it to a object of bytes. The output will result in a form, that looks like a key.

*f018bf984e6b70793d51404c9aa28a29b3c93293334822f6a73cd1a912b47b48*

By using it as a key to decipher AES-256 ECB encrypted text.

Flag: **ECSC{Ne6r0nNetsAreCr1zyANdTerm1nat0r}**



ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str.
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece