October 2022

D

ECSC 2021 – Prague

**Challenge author:** Filip @ *SkylonHost*

Writeup for challenge ENHANCE!

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](mailto:ecsc@enisa.europa.eu)  
For media enquiries about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

Authors/acknowledgements

John Smith, European Union Agency for Cybersecurity

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](#_Toc117433189)

[1.1 Challenge specification 3](#_Toc117433190)

[1.2 Technical Specification 3](#_Toc117433191)

[1.2.1 Required infrastructure 3](#_Toc117433192)

[1.2.2 Provided files 3](#_Toc117433193)

[2. Attack Scenario 4](#_Toc117433194)

[2.1 Description of the scenario 4](#_Toc117433195)

[2.2 Installation Instructions 4](#_Toc117433196)

[2.3 Tools needed for solving the challenge 4](#_Toc117433197)

[2.4 Walkthrough (Writeup) 4](#_Toc117433198)

1. Information regarding the challenge

## Challenge specification

* Challenge Category: Forensics
* Difficulty: Medium
* Expected time to solve: 3h

## Technical Specification

### Required infrastructure

No infrastructure is required to prepare the challenge. Solving can be done offline.

### Provided files

Figure 1: List of files

|  |  |  |  |
| --- | --- | --- | --- |
| File name | Format | Comment | Checksum (SHA256) |
| decode.py | Python script | Solver script by author | 51c0d68638d9385d8d9e40cd6c2bae3585b9259c26fa4733e0411c57172ba0f6 |
| ecsc\_enhance3.pcap | PCAP file | Challenge | 4cfe1ffae44c879fadbe0dc99869be53bd200c38b4e97f290f368ea850d4a637 |

1. Attack Scenario

## Description of the scenario

Challenge is about finding out all images from PCAP dump and modifying them inside some Graphics processor to combine them to get the flag from resulting image.

## Installation Instructions

You only need to distribute the file **ecsc\_enhance3.pcap** to the contestants.

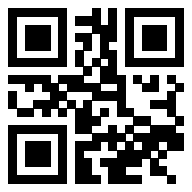
## Tools needed for solving the challenge

Needed tools are:

* Wireshark
* Graphics processor (GIMP, Photoshop etc.)

## Walkthrough (Writeup)

1. Use provided decode.py script to get everything you need to get the flag.
   1. The script will iterate and get all ICMPv6 destination addresses and will reconstruct all images by using coordinates and RGB-triplets from addresses.
   2. Images are saved to the folder
   3. Each image can be edited to be read better – XOR, brightness and other techniques
   4. Images can be combined in Graphics processor
   5. Edit each image’s opacity to get the flag.
2. Flag:  
   **ECSC{e99565674c223c064beff0d68303ec7f}**



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