The Framework Programme for Research & Innovation

Innovation actions (IA)

Project Title:

Cyber Security Accelerator for trusted SMEs IT Ecosystems

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under Grant Agreement n°740690

FORTIKA Challenge #1

Attack to an asset located behind a FORTIKA Gateway

Code of Honor: Respecting the sportsmanship spirit and the rules for a fair game, the players are kindly requested:

- to not perform (D)DoS attacks towards the Asset.
- to not deactivate (e.g shut it down or put it offline) the Asset after capturing the flag.

In addition, all CTF rules as referred in:
https://www.ecsc.gr/files/ECSC_2020_GreekQuals_CTF_Brief.pdf apply to this challenge

Description: This challenge aims on enabling the hackathon participants to capture the flag by exploiting vulnerabilities of an Asset placed behind a FORTIKA GW. In the FORTIKA GW, an IDS (Intrusion Detection System) developed in the project will have been deployed (as the name implies detection and no blocking activities will be performed/triggered by the IDS). After the hackathon's ending the IDS logs will be analysed towards gaining insight that will help the project to improve the IDS solutions capabilities.

The players will have in their availability the IP address (62.171.143.3) of the Asset and the description of the flag that they must capture from the targeted Asset for claiming victory.

Using the Asset's address information, the players have to discover/identify the services offered from the Asset, find out about their possible vulnerabilities, exploit any of them and as such gain access to the Asset (e.g root shell) for retrieving the flag. The flag will be in a file named "fortika-flag.txt" placed in the /root directory. Upon retrieving the file, the players have to identify the encoding used to protect the file's content and decode it.

To claim victory the players have to send the decoded content to the email: fortika.challenges@gmail.com including in the email subject their email account (the one they use to login in the CTF platform: https://ctf.hackthebox.eu/login).

In a nutshell:

- Information:
  - Asset IP : 62.171.143.3
  - Flag: /root/fortika-flag.txt
- Objective:
  - Retrieve the flag file from the asset.
  - Decode the content of the flag file
- Victory claim:
- Send the decoded content to the email: fortika.challenges@gmail.com including in the email subject their email account (the one they use to login in the CTF platform: https://ctf.hackthebox.eu/login).