CTF - Reverse Engineering using Ghidra

Downloaded from hackaday.io - AND!XOR DC27 Badge

This Capture the Flag (CTF) can be done anywhere since it is a downloadable file. We are using the prebuilt reversing challenge from:

hackaday.io/project/164346-andxor-dc27-badge/log/164366-reverse-engineering-with-ghidra-simtaco-floppy-challenge.

The Challenge… Using Ghidra. Capture all the flags you can, identify and exploit as many vulnerabilities as you can, write a report, and write a walk through on how you found each item within. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents. Feel free to use the hackaday link for a reference, just write your own from scratch.

Winner will have their report and walkthrough showcased in a future issue of the Cyber Intelligence Report (CIR) & win a commemorative Litetcoin challenge coin (Not a real Litecoin). This will also be added to the CSI Linux Tutorials section. Submit report and walkthrough to: CTF@informationwarfarecenter.com.

Preferably, use CSI Linux Analyst (csilinux.com/download.html). Ghidra is already installed. The Simtaco file is a Linux executable.

Deadline: September 15th, 2020!

To compete, you must sign up here:
comms.informationwarfarecenter.com/?p=subscribe&id=3

This is a capture the flag. Even though it has been done before at a conference, it is good practice on a fun challenge. Once you download and install Ghidra, use it to crack the "simtaco" application challenge. Write your own content and do not plagiarize from other work. That is the only real rule.

Scenario

You find a Linux binary that looks interesting. First step:

- chmod +x the binary to make it executable
- Run the file
- Crack the app

For hints, you can visit:
hackaday.io/project/164346-andxor-dc27-badge/log/164366-reverse-engineering-with-ghidra-simtaco-floppy-challenge

Remember: Score is based off the quality of the report and walkthrough.

RE CTF TARGET DETAILS

Download the file here:

http://bit.ly/2EQMHgH
Backup Link

- Filename: simtaco
- File size: 12.6k
- MD5: 872A8AF58B274D4022DF7E394FCEB46C
- SHA1: 49D7FCE1551D1D1DF5210C7DB19983153D8CF4D5

Ghidra (Java 11 Required)

- Download ghidra-sre.org

CSI Linux: (VirtualBox Required)

- Download CSI Linux

Additional Resources

- Ghidra Guide (Official)
- Ghidra Guide – Ghidra.re