RTU Vulnerability Analysis Demonstration using a vulnerable virtual RTU (vvRTU)

BACKGROUND:
This project uses docker-containers for the development, configuration, and installation of the vulnerable virtual remote terminal unit (vvRTU) in a laboratory setup. The existing Linux-based container has to be extended by including versioned services with known vulnerabilities. The demonstration should make use of the general testing framework metasploit (MSF) to develop a full host compromise and functional modification of the target service with remote access. The produced artefacts are a customized MSF-exploit script, machine-readable specification of the vvRTU as versioned source code, alongside a thesis paper written according to scientific standards and guidelines at Department II of Uni Oldenburg. One key artefact will be the detection and countermeasures of the implemented vulnerabilities.

OBJECTIVE:
The objective of this thesis is to demonstrate the compromise of an RTU demonstrator in the OFFIS SESA-Lab. The striving hacker should setup the vvRTU and demonstrate how the compromise of one common service leads to compromise of a critical target service running on the vvRTU. Detections, Countermeasures and threat models will also be one objective.

YOUR PROFILE:
> We expect the student to bring sufficient experience with fundamental programming languages, especially C to understand and modify existing processes.
> Basic abilities to handle the scripting language Ruby have to be acquired.
> Technical curiosity and a “security mindset” are crucial.
> Clean Code Development and documentation processes are mandatory.

OUR OFFER:
> You will have the opportunity to gain experience as a security researcher and participate in interesting and innovative international project.
> You will be supported by cyber security expert and a team of researchers from various scientific fields as well as technical infrastructures of the Smart Energy Simulation and Automation (SESA) laboratory.
> A pleasant working environment within a highly competent and international team.

If you are interested, please simply write an e-mail to the address below.

CONTACT AND SUPERVISION:
Dr.-Ing. Jirapa Kamsamrong
OFFIS - Institute for Information Technology, Escherweg 2, 26121 Oldenburg
Mail: jirapa.kamsamrong@offis.de