OTLab 02

Siemens S7 PLC Emulation

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

Warning: The tasks in this document are strictly educational, observational, and non-intrusive, and must fully comply with ethical and legal standards.

Tasks

1. Verify the IP address of the `otlab-student` workstation.
2. Determine the subnet range of the network where the `otlab-student` workstation is deployed.
3. Discover the IP address, MAC address, and vendor information of other active hosts within the network. *Hint: It is a PLC*.
4. Identify open ports and available services on the OT-ICS host over both TCP and UDP protocols.
5. Determine the proprietary industrial communication protocol used by the PLC.
6. Retrieve additional system information using vendor-specific `nmap` scripts.
7. Execute a plcscan on the OT-ICS device detected on the network and collect further data.

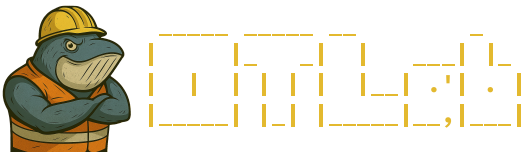
Note: On the `otlab-student` workstation, the `opt/plcscan/plcscan.py` tool (meeas/plcscan) must be executed using `python2`.

Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 02: `ifconfig`, `masscan`, `netdiscover`, `nmap`, and `plcscan`.

Nomenclature

- ICS: Industrial control system.
- IP: Internet protocol.
- MAC: Media access control.
- OT: Operational technology.
- PLC: Programmable logic controller.



- TCP: Transmission control protocol.
- UDP: User datagram protocol.