OTLab 01

Basics of OT-ICS Devices Discovery

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

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

Warning: When using specialized search engines or Google dorks to identify Internet-exposed OT devices, do not interact with or attempt to access any real systems. 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 via the SNMP protocol.
7. Identify the total number of publicly accessible OT-ICS devices using the same proprietary industrial protocol as `conpot-plc` through a specialized search engine such as Shodan or FOFA.
8. Locate a publicly exposed OT device using the same industrial protocol as `conpot-plc` through Google dorking.

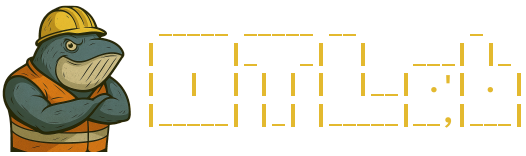
Note: The `conpot-plc` is based on Conpot, which remaps standard protocol and service ports to non-privileged ports. Refer to the link for a list of some default and remapped ports.

Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 01: `ifconfig`, `masscan`, `netdiscover`, `nmap`, and `snmpwalk`.

Nomenclature

- ICS: Industrial control system.



- IP: Internet protocol.
- MAC: Media access control.
- OT: Operational technology.
- PLC: Programmable logic controller.
- SNMP: Simple network management protocol.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.