OTLab 03

Emulation of a Gas Station Control System

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

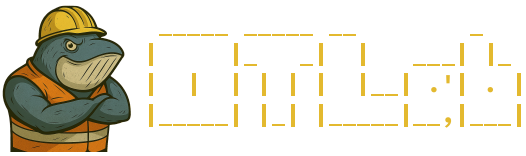
1. Verify the IP address of the `otlab-student` workstation.
2. Determine the subnet range of the network where the `otlab-student` workstation is deployed.
3. Discover the IP address, MAC address, and vendor information of other active hosts within the network. *Hint: One of the devices is an automatic tank gauge (ATG) controller.*
4. Identify open ports and available services on the OT-ICS host over both TCP and UDP protocols.
5. Retrieve additional system information using vendor-specific `nmap` scripts.
6. Identify the total number of publicly accessible OT-ICS devices using the same open port as `gas_station` through a specialized search engine such as Shodan or FOFA.
7. Determine the total number of publicly exposed OT-ICS devices that implement the same ATG-related functionality as the `gas_station` host by querying a specialized search engine such as Shodan or FOFA.

Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 03: `ifconfig`, `masscan`, `netdiscover`, and `nmap`.

Nomenclature

- ATG: Automatic tank gauge.
- ICS: Industrial control system.
- IP: Internet protocol.



- MAC: Media access control.
- OT: Operational technology.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.