OTLab 05

Modbus/TCP Routing Between Subnets

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

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

Tasks

1. Verify the IP addresses assigned to the `otlab-student` workstation.
2. Determine the subnet ranges of the networks in which the `otlab-student` workstation is deployed.
3. Discover the IP address, MAC address, and vendor information of other active hosts within the subnets. *Hint: Two industrial devices belong to the same vendor.*
4. Identify open ports and available services on both OT-ICS hosts over TCP and UDP protocols.
5. Intercept the communication between the OT-ICS hosts and determine the secret message being transmitted. *Hint: The message must be decoded.*

Tools

These are the tools available on the `otlab-student` workstation for completing OTLab 05: `ifconfig`, `masscan`, `netdiscover`, `nmap`, and `tcpdump`.

Nomenclature

- ICS: Industrial control system.
- IP: Internet protocol.
- MAC: Media access control.
- OT: Operational technology.
- TCP: Transmission control protocol.
- UDP: User datagram protocol.