OTLab 06

Industrial Protocols and Web Interface Exposure

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

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

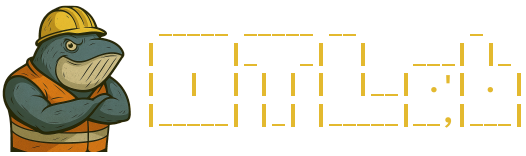
Tasks

1. Verify the IP address of the `otlab-student` workstation. `OTLab06{XXX.XXX.X2.XXX}`
2. Discover the IP addresses of the active hosts within the same subnet as the answer above. `OTLab06{XXX.XXX.XX.2X, XXX.XXX.XX.XX, XXX.XXX.XX.XXX}`
3. Determine which ports are open on the IP address in the format `XXX.XXX.XX.2X`, identified in the previous question. `OTLab06{XXXX, XXXX, XXXX, XXXXX, XXXXX}`
4. Identify the MAC address of the active host corresponding to the IP address in the format `XXX.XXX.XX.2X` from Question 2. `OTLab06{XX:XX:XX:XX:XX:XX}`
5. Locate the hidden flag within a web interface exposed on the active host mentioned in Question 3. *Hint: Use curl. No further hints provided*.
6. Which port is open on the IP address in the format `XXX.XXX.XX.3X` from Question 2? `OTLab06{XXX}`
7. Determine the version of the basic firmware emulated on the active host referenced in the previous question. `OTLab06{X.X.X.X}`
8. Two devices on distinct networks configured in bridge mode are communicating. What is the MAC address of the sole active host on the other bridged segment? `OTLab06{XX:XX:XX:XX:XX:XX}`
9. Two devices on distinct networks configured in bridge mode are communicating. What is the transmitted message? `OTLab06{Xxxx xxx Xxxxxxxxxxx xx Xxxxxxxx xxx Xxxxxxxxx xxx XX-XXX!}`
10. Which OID can be extracted via the SNMP service from an active host operating with an industrial communication protocol? `OTLab06{OID: ...}`

Note: The `plc03-scada` 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. 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 06:



`ifconfig`, `masscan`, `netdiscover`, `nmap`, `snmpwalk`, `plcscan`, and `tcpdump`.

Nomenclature

- IP: Internet protocol.
- MAC: Media access control.
- OID: Object identifier.
- SNMP: Simple network management protocol.