Automatic OT Pentest Report

Automatic OT Pentest tool

June 24, 2024

Contents

1 Summary of report

A summary of modules that found something of interest. This list may not include all modules executed.

Each module is given a risk score based

- Modbus host discovery: Discovers hosts running Modbus
- Modbus UID discovery: Finds UIDs available on a Modbus host
- SYN scan for open ports: Sends SYN packets to establish a connection and detect open ports

2 Modbus host discovery

Risk: 8

Discovers hosts running Modbus

Mitigation strategies:

- Implement a firewall

- Use a VPN to encrypt communication across networks
- Isolate the Modbus network

Host	Port
127.0.0.1	502
127.0.0.2	502
127.0.0.8	502
127.0.0.4	502
127.0.0.32	502
127.0.0.128	502
127.0.0.64	502
127.0.0.16	502

3 Modbus UID discovery

Risk: 10

Finds UIDs available on a Modbus host

Mitigation strategies:

- Implement a firewall
- Use a VPN to encrypt communication across networks
- Isolate the Modbus network

Results from scanning 10 UIDs on 8 hosts:

Host	UID
127.0.0.1	0,1,2,3,4,5,6,7,8,9
127.0.0.2	0,1,2,3,4,5,6,7,8,9
127.0.0.8	0,1,2,3,4,5,6,7,8,9
127.0.0.4	0,1,2,3,4,5,6,7,8,9
127.0.0.32	0,1,2,3,4,5,6,7,8,9
127.0.0.128	0,1,2,3,4,5,6,7,8,9
127.0.0.64	0,1,2,3,4,5,6,7,8,9
127.0.0.16	0,1,2,3,4,5,6,7,8,9

4 SYN scan for open ports

Risk: 6

Sends SYN packets to establish a connection and detect open ports

Scanned 500 ports

Mitigation strategies:

- Apply a filter to block malicious traffic
- Enforce whitelisting to prevent unknown devices from connecting
- Close all unused open ports

Host	Port	Status
127.0.0.1	502	Open