Automatic OT Pentest Report

Automatic OT Pentest tool

June 20, 2024

0.1 Modbus host discovery

Severity: 5

Discovers Modbus on hosts

Mitigation strategies:

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

Host	Port
127.0.0.1	502

0.2 UIDs

Severity: 9

Finds UIDs available on a Modbus host

Mitigation strategies:

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

UID
0
2
1
3
4
5
8
7
6
10
9

0.3 SYN scan of open ports

Severity: 3

Sends SYN packets to establish a connection and detect open ports

Mitigation strategies:

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

Scanned 9500 ports

Host	Port	Status
127.0.0.1	502	Open