OT Penetration Testing Report

Date: 2025-11-26 **Target Environment:** Mock OT Network

1. Executive Summary

Overview

An automated penetration test was conducted on the OT environment. The assessment identified critical vulnerabilities that could lead to significant operational disruption, including the ability to stop PLCs and manipulate process control parameters.

Key Risks

- **Operational Disruption**: Confirmed ability to stop Siemens S7 PLCs (DoS).
- **Process Manipulation**: Unauthorized control of Modbus devices (Coil Write).
- **Unauthorized Access**: Default credentials and weak SNMP community strings found.

Strategic Recommendations

1. **Network Segmentation**: Strictly separate IT and OT networks.
2. **Hardening**: Change all default passwords and community strings immediately.
3. **Access Control**: Implement strict IP whitelisting for Modbus and S7 communication.

2. Asset Inventory

192.168.1.10 (Siemens)

- Port 80/tcp: HTTP (Siemens Web Server)
- Port 102/tcp: Siemens S7 Comm (S7-1500 v2.1)
- Port 443/tcp: unknown (unknown)
- Port 502/tcp: Modbus TCP (Simatic Modbus)

192.168.1.20 (Schneider Electric)

- Port 80/tcp: HTTP (Apache 2.4)
- Port 443/tcp: unknown (unknown)
- Port 5900/tcp: VNC (RealVNC 5.3)

192.168.1.30 (Moxa)

- Port 22/tcp: SSH (OpenSSH 8.2)
- Port 80/tcp: unknown (unknown)
- Port 502/tcp: Modbus TCP (Moxa Modbus Gateway)

- **192.168.1.100** (Generic)

3. Technical Findings & Recommendations

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ Exploit Success (CRITICAL)

Asset: 1 | **Source:** MetasploitAgent

Description: Exploited with exploit/multi/http/default*creds*exec. Meterpreter session 1 opened. User: admin (uid=0)

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'stop_cpu' successful. PLC 192.168.1.10 switched to STOP mode. Process Halted.

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ ICS Impact (CRITICAL)

Asset: 1 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Register written. Setpoint changed to 100.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ ICS Impact (CRITICAL)

Asset: 3 | **Source:** IcsAgent

Description: Action 'write_coil' successful. Coil 1 written successfully. Gateway configuration changed.

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Web Vulnerability (HIGH)

Asset: 1 | **Source:** WebScanner

Description: Default Credentials (admin/admin)

■ **Mitigation / TO-BE Recommendations:** - **Password Policy**: Change default passwords immediately. - **MFA**: Implement Multi-Factor Authentication where supported. - **Account Lockout**: Enable account lockout policies to prevent brute force.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ Default SNMP Community String (MEDIUM)

Asset: 1 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Siemens S7-1500 FW:2.1

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ Default SNMP Community String (MEDIUM)

Asset: 3 | **Source:** SnmpScanner

Description: Found default community string 'public'. System: Moxa MGate MB3180

■ **Mitigation / TO-BE Recommendations:** - **Upgrade to SNMPv3**: Use SNMPv3 with authentication and encryption (AuthPriv). - **Change Community Strings**: Replace 'public'/'private' with complex strings. - **ACLs**: Restrict SNMP access to authorized management stations only.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: s7-info (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Module: 6ES7 511-1AK01-0AB0 Basic Hardware: S7-1500 Version: 2.1.0

■ **Mitigation / TO-BE Recommendations:** - **Access Control**: Enable password protection for the S7 PLC (Protection Level 3). - **Network Segmentation**: Isolate the PLC network from the corporate IT network. - **Disable Services**: Disable the web server and PUT/GET communication if not needed.

■ NSE Info: modbus-discover (INFO)

Asset: 1 | **Source:** NmapAgent

Description: Sid: 1 Device: Simatic Modbus TCP

■ **Mitigation / TO-BE Recommendations:** - **Firewall Rules**: Whitelist authorized IP addresses (e.g., SCADA Master) for Modbus TCP (Port 502). - **VPN**: Use VPNs for remote access to the OT network. - **PLC Logic**: Implement logic to validate write commands or use specific Modbus function code filtering.

■ NSE Info: ssh-auth-methods (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Supported: publickey, password

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.

■ NSE Info: modbus-discover (INFO)

Asset: 3 | **Source:** NmapAgent

Description: Sid: 1 Device: Moxa NPort

■ **Mitigation / TO-BE Recommendations:** - **General**: Patch the system and restrict network access.
