Penetration Testing Report

Executive Summary

This report presents the findings of a comprehensive network security assessment conducted on the OT (Operational Technology) network. The assessment aimed to identify potential vulnerabilities and security gaps within the network infrastructure. The findings highlight several critical issues that require immediate attention to mitigate the risk of unauthorized access and potential disruptions to operational processes.

Key Findings

1. **Flat OT Network Architecture:**
    - The entire OT network operates on a flat architecture, where all hosts are connected within a single network segment. This design lacks segmentation, increasing the risk of lateral movement and unauthorized access to critical systems.
2. **Undocumented Remote Access Router:**
    - An undocumented remote access router was discovered, allowing external third parties to access the client's OT network without proper access controls. This presents a significant security risk as it could lead to unauthorized access to sensitive systems and data.
3. **Misconfigured Webserver of Siemens S7-1500:**
    - The web server of the Siemens S7-1500 device is misconfigured, allowing unauthorized individuals to toggle the CPU state from RUN to STOP. This could potentially cause production stoppages and disrupt operations.

Figure 1: CPU operator panel of Cookie Line's PLC

4. **Misconfigured Oven Control HMI:**
    - The Oven Control HMI (Human-Machine Interface) is misconfigured, enabling unauthorized individuals to alter oven settings or shut down the oven altogether. This poses a risk to production processes and could lead to operational disruptions.

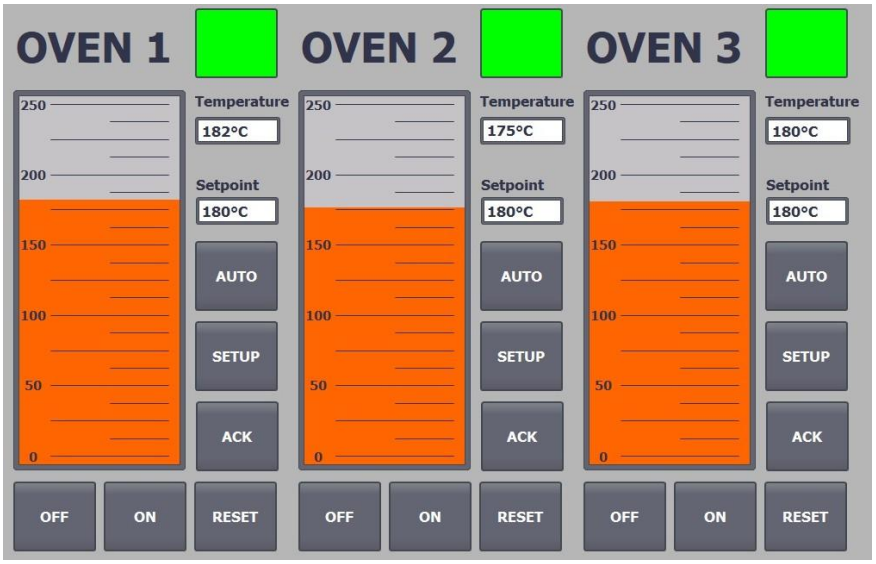

Figure 2: Unprotected Oven Control HMI

5. **Commonly Used TCP Ports:**
    - Port 102 is utilized by six devices using the Siemens S7 industrial protocol, indicating potential vulnerabilities associated with this widely used protocol.
    - Port 80 is used by devices hosting remote control web services, suggesting the presence of externally accessible services that may be susceptible to exploitation.

Identified Risks

1. **Risks of a flat OT network:**
    - **Description:** All devices are connected to a single network segment, presenting several vulnerabilities including multiple entry points for attackers, increased risk of unwanted software (malware/worms) spreading to connected systems, and a single point of failure.
    - **Impact:** Potential compromise of critical operational systems, data loss, and disruption of production processes.
2. **Risk of undocumented VPN Router:**
    - **Description:** Lack of documentation and control over a VPN router introduces vulnerabilities such as no access control over third parties, inadequate management of device updates and account policies, and potential exposure of OT equipment to the cloud or the internet.

- **Impact:** Increased risk of unauthorized access, data breaches, and potential exploitation by malicious actors.

3. **Risk of exposed PLC and HMI remote control functions:**

- **Description:** Exposed PLC (Programmable Logic Controller) and HMI (Human-Machine Interface) remote control functions pose the risk of unauthorized access and manipulation of processes.
- **Impact:** Potential for unauthorized control, manipulation, or disruption of industrial processes, leading to operational downtime.

Mitigations

1. Mitigating VPN Router Risk:

Enforce Strong Access Controls:

- Apply multi-factor authentication (MFA).
- Restrict VPN access to authorized personnel only, using RBAC.

Patch Management:

- firmware updates and security patches regularly.

Isolate and Log VPN Access:

- Place VPN behind a DMZ.
- Log all remote connections and monitor for anomalies.

2. Mitigating Unauthorized HMI Access:

To mitigate unauthorized access to the Human-Machine Interface (HMI), the following strategies should be implemented:

Restrict Remote Access:

- Disable unnecessary remote access features on PLCs and HMIs.
- Allow only read-only access for monitoring where possible.

Access Controls and Audit Logging:

- Enforce authentication (no default or hardcoded passwords).
- Enable access logs and review regularly.

3. Mitigating the Flat OT Network:

Implement Network Segmentation:

- Deploy firewalls and VLANs to separate zones (e.g., Level 0-3 per Purdue Model).
- Apply zone/conduit model as per IEC 62443-3-2.

Introduce Demilitarized Zones (DMZs):

- Create a buffer zone between IT and OT to control data flow (historian, patching services, etc.).

4. General Recommendation: Defense in Depth

It is recommended to implement a defense-in-depth strategy, which involves layering multiple security measures throughout the network infrastructure. This approach ensures that even if one security measure fails, others are in place to provide protection.

Assessment Methodology

The assessment was conducted using a systematic approach to identify vulnerabilities and potential security risks within the OT network. The following methodology was employed:

- **Tools:** Netdiscover and Nmap tools were used for host discovery and enumeration.
    - Netdiscover was utilized for Layer 2 discovery to identify devices within the network.
    - Nmap was employed for Layer 3 discovery to determine the availability of devices and services.
- **Netdiscover:** A Layer 2 Arp-Discovery Scan was used to identify devices, their MAC Address, IP Address and Vendor Data based on the device.
- **Nmap Ping Sweep:** A Nmap ping sweep was conducted to identify devices responding to ICMP echo requests, indicating active hosts within the network. Responding devices were further analyzed.
- **Nmap Port Scan:** A Nmap port scan was conducted to identify open ports on devices marked as safe to scan.
- **Nmap Scripting Engine:** The Nmap Scripting Engine was utilized to extract device information from a Siemens Simatic S7-1500 Industrial Controller.

```
PORT    STATE SERVICE
102/tcp open  iso-tsap
| s7-info:
|   Module: 6ES7 511-1AK01-0AB0
|   Basic Hardware: 6ES7 511-1AK01-0AB0
|   Version: 3.2.6
|   System Name: PRODUCTION S7-1500
|   Module Type: CPU 1511-1 PN
|   Serial Number: S C-H3SF38492016
|_  Copyright: Original Siemens Equipment
MAC Address: 00:1C:06:1C:BD:11 (Siemens Numerical Control, Nanjing)
Service Info: Device: specialized
```

Figure 3: s7-info.nse output

Conclusion

The findings of the network security assessment underscore the importance of addressing critical vulnerabilities and implementing robust security measures within the OT network. Immediate action is required to remediate the identified issues and enhance the overall security posture of the network. Failure to address these vulnerabilities could result in severe consequences, including operational disruptions, data breaches, and compromise of sensitive systems.

These mitigation recommendations aim to enhance the security posture of the OT network, safeguarding against unauthorized access and potential threats. Implementation of these measures should be prioritized to mitigate risks effectively and ensure the integrity and confidentiality of critical assets.