Penetration Testing Report

Executive Summary

This report presents the findings of a comprehensive network security assessment conducted on the OT (Operational Technology) network of [Client Name]. 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. (See appendix)
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. (See appendix)
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.

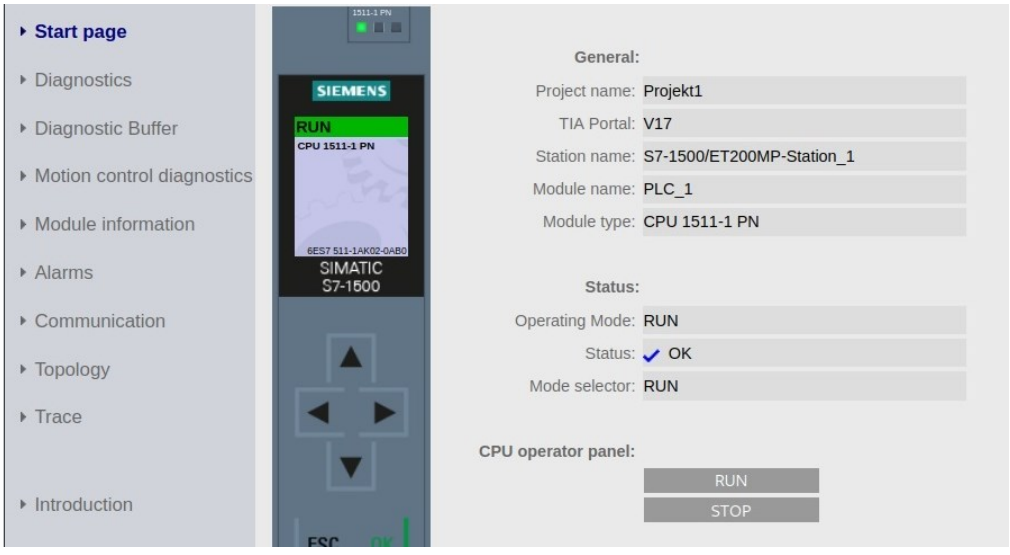

Figure 1: CPU operator panel of Cookie Line's PLC

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.

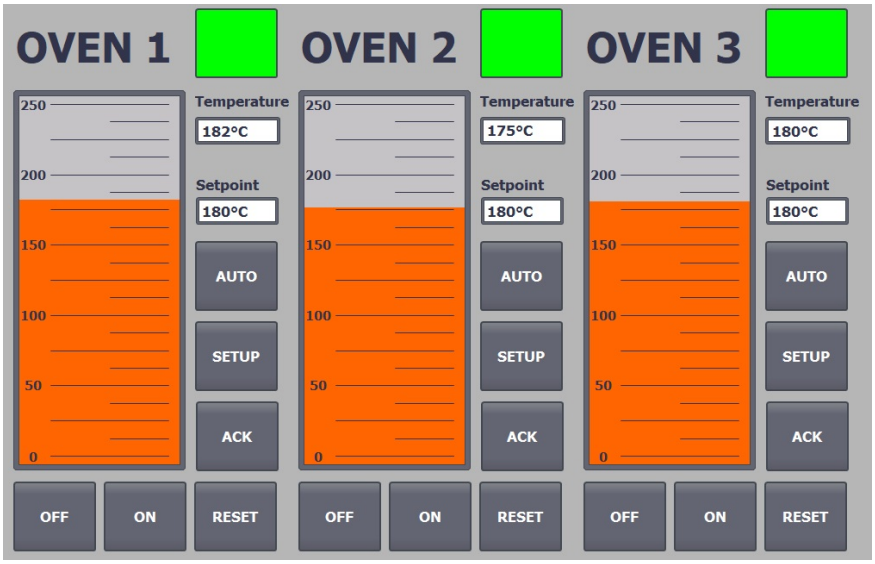

Figure 2: Unprotected Oven Control HMI

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.
    - **ICS ATT&CK Techniques:**
        - Discovery (T878): Attackers may exploit the flat network structure to identify and map out devices and entry points.
        - Exploitation for Defense Evasion (T811): Attackers may leverage the lack of segmentation to evade detection and spread malware.
        - Impact (T829): Attackers can exploit the single point of failure to disrupt or halt operations.
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.
- **ICS ATT&CK Techniques:**
    - Initial Access (T1078): Attackers may exploit undocumented VPN routers as entry points into the OT network.
    - Exploitation for Privilege Escalation (T826): Attackers could leverage insufficient access controls and policies to escalate privileges and gain unauthorized access.
    - Exfiltration (T1041): Attackers may exploit the lack of control over network traffic to exfiltrate sensitive data.

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.
- **ICS ATT&CK Techniques:**
    - Command and Control (T1001): Attackers may exploit exposed remote control functions to establish command and control over industrial processes.
    - Impact (T829): Unauthorized manipulation of PLC and HMI functions may lead to disruptive impacts on operational processes.
    - Exploitation for Impact (T1485): Attackers may exploit exposed remote control functions to directly impact operational processes.

Mitigations

1. Mitigating Unauthorized PLC Webserver Access:

To address unauthorized access to the PLC webserver, the following measures are recommended:

- **Access Protection:** Implement access protection mechanisms for both the webserver and the device display to prevent unauthorized entry.
- **Read-Only Access:** Configure the webserver with read-only access rights to restrict modifications and ensure data integrity.
- **PLC Access Level Setting:** Set the PLC Access Level to HMI to control access more effectively.

2. Mitigating Unauthorized HMI Access:

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

- **Disable Remote Control Runtime Services:** Disable remote control runtime services to prevent unauthorized access attempts.
- **Password Policy Enhancement:** Enforce stricter password rules requiring a minimum of 9 characters, including at least one number, to enhance password security.
- **User Segmentation:** Introduce User Segmentation by creating Administrative User Groups and Operative User Groups to limit access based on roles.
- **Control Screen Segregation:** Implement Control Screen Segregation by categorizing access into two levels: 1. Displaying Information only, and 2. Access to oven control functions, to restrict access to critical functionalities.

3. Mitigating the Flat OT Network:

To address the risks associated with a flat OT network architecture, the following steps should be taken:

- **Next-Generation Firewall Implementation:** Deploy a next-generation firewall to establish a DMZ (Demilitarized Zone) and VLANs (Virtual Local Area Networks) within the OT network.
- **Network Segmentation:** Apply network segmentation techniques as recommended in the provided attachment to enhance network security and isolate critical assets from potential threats.

4. Mitigating the Undocumented VPN Access Router:

To mitigate the risks posed by an undocumented VPN access router, the following actions are proposed:

- **Move Device to DMZ:** Relocate the VPN access router to the DMZ to facilitate firewall control over network communication and enhance security.
- **Network Communication Restrictions:** Restrict all network communication except for specific hosts listed in the firewall allow list to minimize unauthorized access.
- **Internal Personnel Activation:** Enable activation of the VPN tunnel only by internal personnel, forbidding external activation to prevent unauthorized entry.
- **Personalized Accounts:** Require the service provider to use personalized accounts for VPN access to enhance accountability and traceability.

5. 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 MAC (See appendix).
- **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 (See appendix).
- **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.

For any further assistance or clarification, please do not hesitate to contact us.

Sincerely,

[Your Name]
[Your Position/Title]
[Your Contact Information]