Industrial attack scenario

Let us assume that an external attacker (threat actor) was able to get access to the internal production network and is now able to directly access all available devices. The example scenario is shown in Fig. 1 in a simplified version.

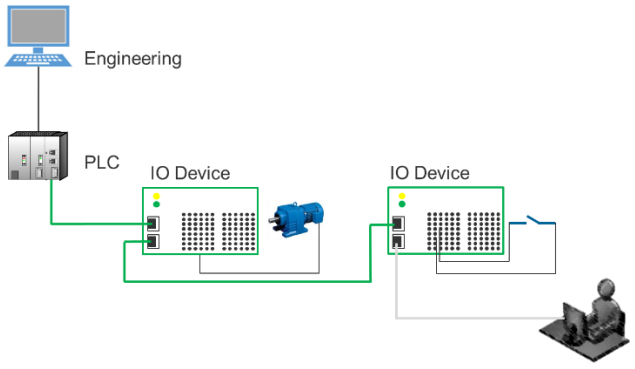

Fig 1. Simple attack scenario of an industrial control system

Preparation

Startup the installed Kali Linux on your Desktop PC in the CIIT Computerlab and login using the standard credentials (User: root, PW: groot). As soon as you are logged in, configure the internal network interface (eth0) with an IP address in the network 192.168.16.0/24. The last octet should be derived from the number which is on your Desktop PC (see this pdf in ILIAS). The network 192.168.16.0/24 is considered as the internal production network.

Exercises

1. Discover the network for available devices and, if possible, services. What are you able to find? 192.168.16.3 (Sean) & 192.168.16.100 (Server)

2. Try to find common vulnerabilities for the devices of your automation network and describe them shortly. weak password, old os/firmware, No network bulfercation, No encryption, No monitoring, firewall

3. Exploit one of the vulnerabilities by using an existing Metasploit module.

4. Analyse the exploitation in detail using Wireshark. What has been used as the main attack vector and how is the vulnerability actually exploited?