**Cyber Attack on OT-PLC-Railway System**

**Introduction**

This project will show the steps to demo two kinds of cyber attack situation on the OT-PLC-Railway system.

**False Data Injection Attack**: When the attack happens, the reversed user control commend will be injected into the system and the exception situation is not detectable from the SCADA HMI system. (When the user try to turn on the Runway lights in the airport, all the runway lights will be turn off.)

**Black Out Attack**: This is one attack situation of Black Energy 3 cyber attack. When the attack happens, all the PLC output coils (energy output) will be turned off. The system HMI center energy may detect the exception situation but the user cannot recover to normal situation by using the SCADA PC. (The SCADA HMI shows everything normal when the user tries to do recover action but actually all the related PLC output will still keep turned off state)

**Attack Demo**

Step 1 Hardware power check

* 1. Make sure the OT platform’s power has been turned on and all 3 PLC works normally.
  2. Make sure the technical PC, orchestrator PC and the HMI PC are working normally.

Login Information (username/password):

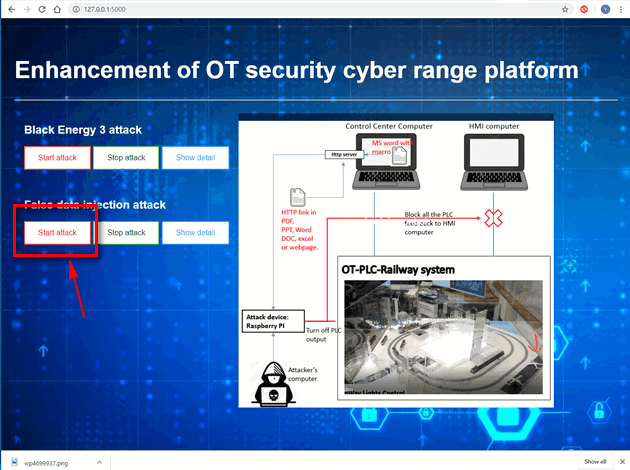
* Technical PC: admin/Qazqwerty123
* HMI PC: root/Qazqwerty123
* Orchestrator PC: 00000000/00000000 => orchestrator/Qazqwerty123
  1. Make sure the attack device (Raspberry PI) is also powered up. (The Raspberry PI green light is on.)

Step2 Demo False data injection attack

2.1 Turn on and off the Runway light to show the control works normally, leave the runway light at turn on state.

2.2 Login the orchestrator PC, open the browser and type in URL:

<http://localhost:5000> or <http://127.0.0.1:5000> and the attack control page will show as below. Press the red color “Start attack” button (marked in the red rectangle).



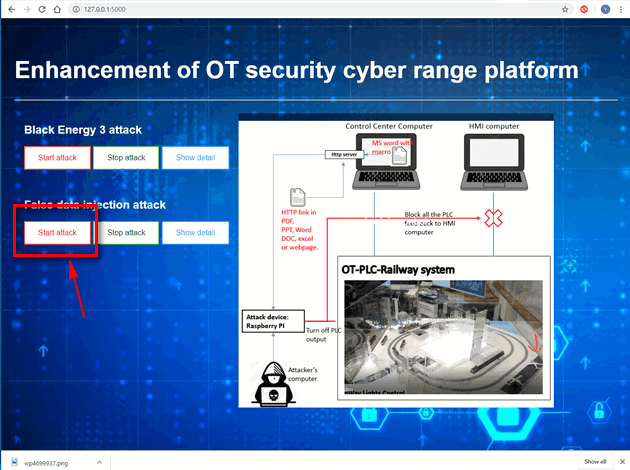
2.3 After 10 ~ 20 seconds, when the runway light turns off which means the false data injection attack was started successfully. Try to turn on/off the runway light from the training HMI and you can see the control signal was reversed.

2.4 Press the green color “Stop attack” button and after 20~30 second when the Run way lights is same as the state shown on the HMI which means the attack has been stopped. Turn on and off the runway light to show the HMI control was recovered.

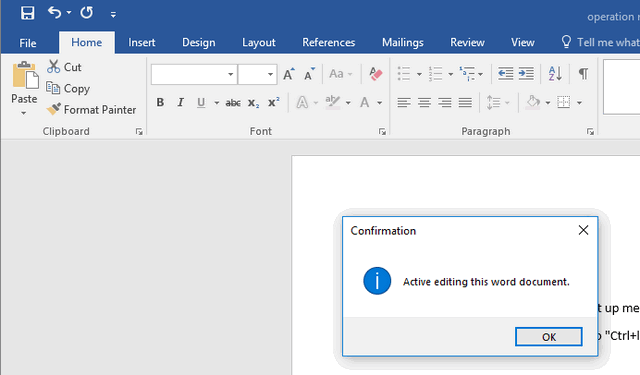
Step3 Demo Back Out Attack

3.1 Turn on all the PLC output to show people the system is working normally.

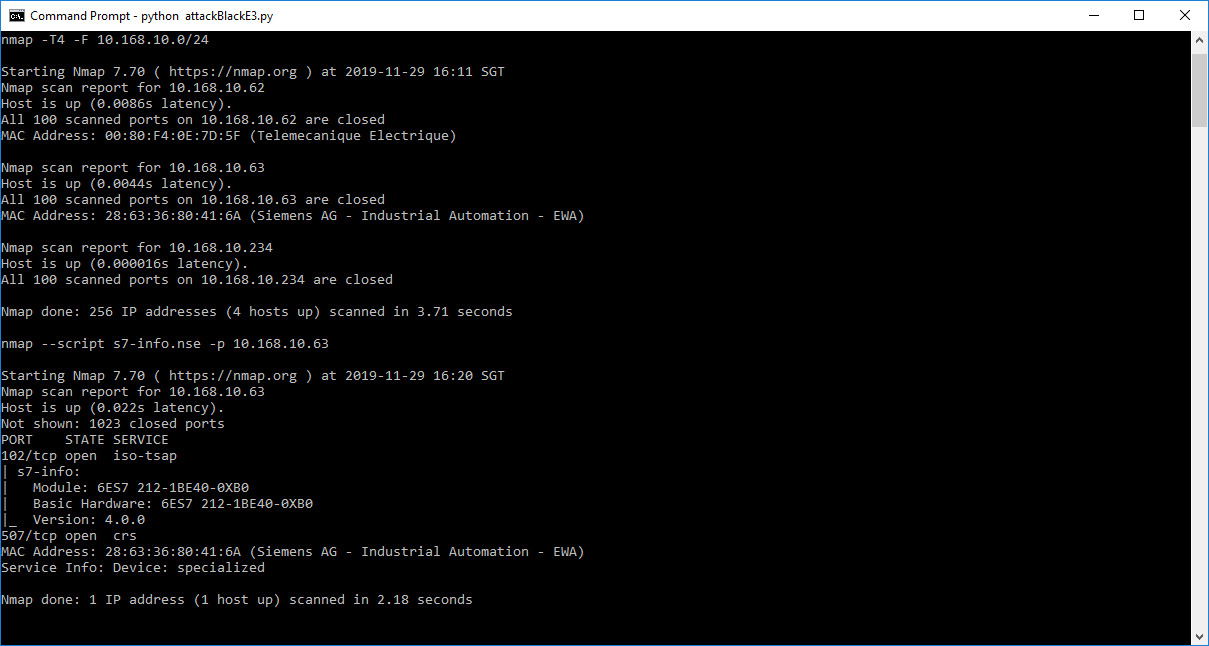
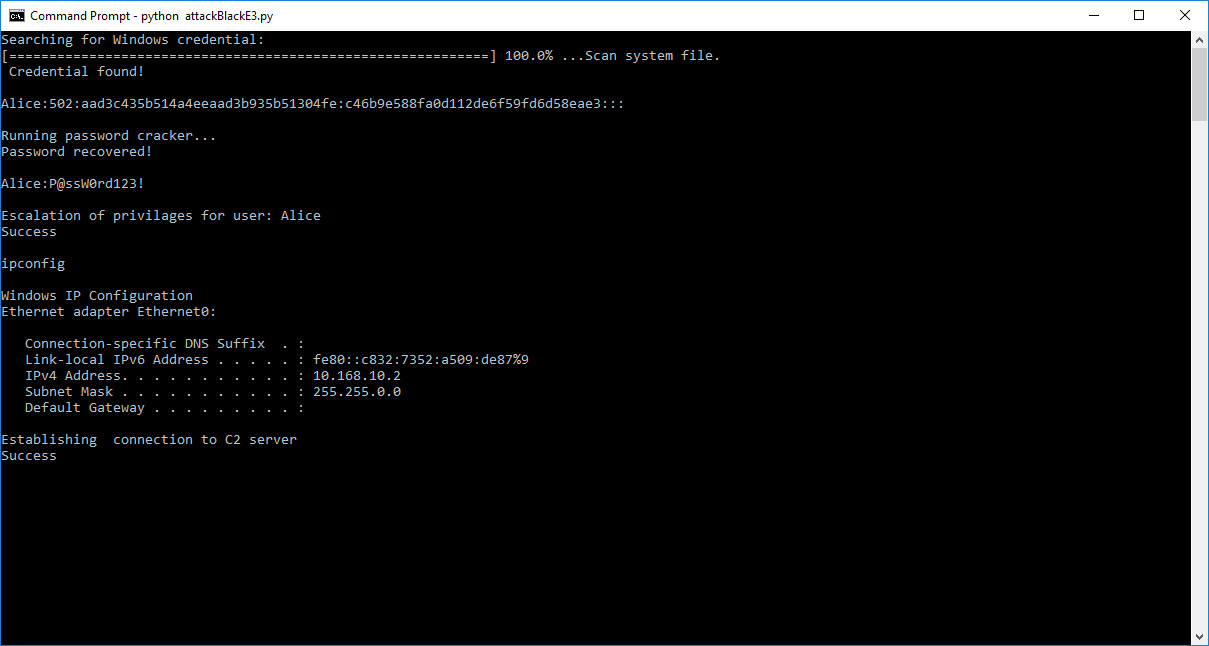
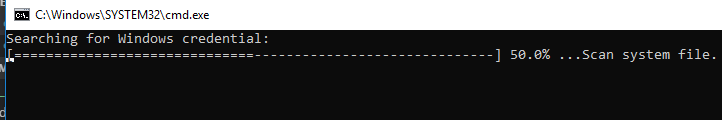
3.2 Same as step\_2.2, Press the red color “Start attack” button under the Back Out Attack.



3.3 After 5 ~ 10 seconds, a word document will open automatically on the technical PC. Press the OK button in the edit enable pop-up window. (As shown below)



The attack detail information will show as below:



3.4 After the program finished running. All the PLC output will be turn off, press the HMI control button to show people the HMI can not control the system.

3.5 Press the green color “Stop attack” button and after 20~30 second the system control will recover.