**OT-PLC-Railway Platform Cyber Attack Implementation Menu**

**Introduction**

This menu will introduce the steps to show two kinds of cyber attack (False Data Injection Attack and Black Out Attack) demo on the OT-PLC-Railway platform.

**False Data Injection Attack**: When the attack happens, the reversed user’s control commend will be injected into the system communication channel and the exception situation will not be detectable from the SCADA HMI. (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 kind of Black Energy 3 cyber attack. When the attack happens, all the PLC output coils (energy output) will be forced turned off. The system HMI may detect the energy system exception situation but the user cannot recover system to normal situation by using the SCADA HMI. (The SCADA HMI shows the system still controllable when the user tries to do recover action but actually all the related PLC output will still keep turned off state.)

**Steps to Show Attack Demo**

**Step 1 - Hardware power check**

* 1. Make sure the OT platform’s power has been turned on and all 3 PLC are working normally.
  2. Make sure the technical PC, the orchestrator PC and the HMI PC are working normally. Login Information (username/password):

Technical PC: admin/Qazqwerty123

HMI PC: root/Qazqwerty123

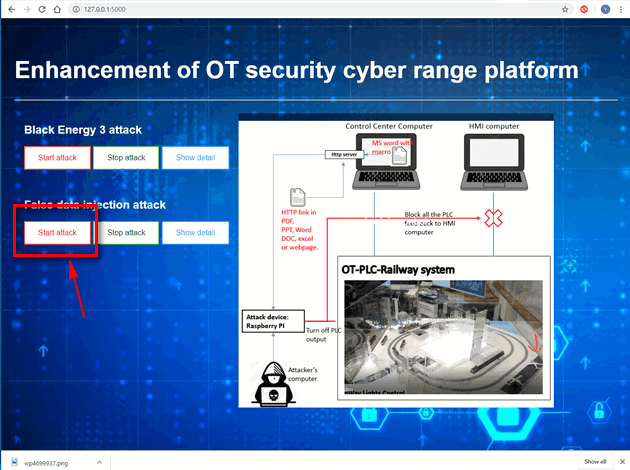
Orchestrator PC: 00000000/00000000 => orchestrator/Qazqwerty123

* 1. Make sure the attack Raspberry PI is also powered up. (The Raspberry PI green light is on.)

**Step 2 – Show false data injection attack demo**

2.1 Turn on and off the airport runway light to show the HMI control works normally, leave the runway light at turn on state for the next step.

2.2 Login the orchestrator PC, open web 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 false data injection attack section red color “Start attack” button (marked in the red rectangle).



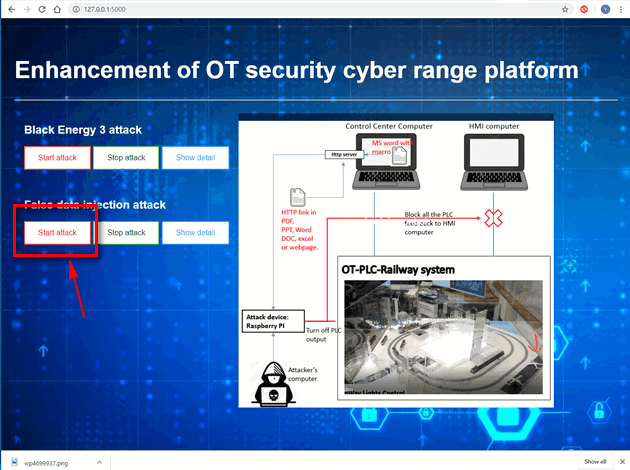
2.3 After 10 to 20 seconds, when the airport runway light turns off which means the false data injection attack has been started successfully. Try to turn on/off the runway light from the training HMI and you can see the control signal has been reversed.

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

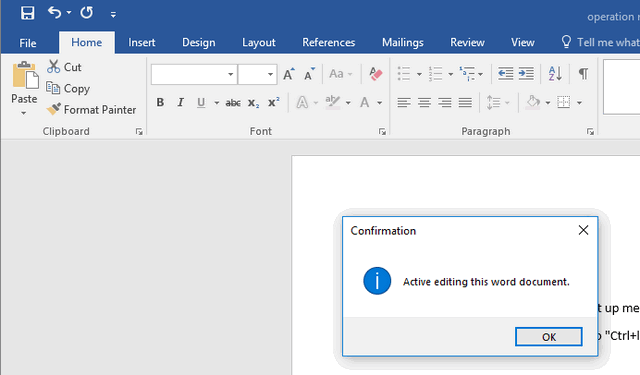
**Step 3 – Show Back out attack demo**

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

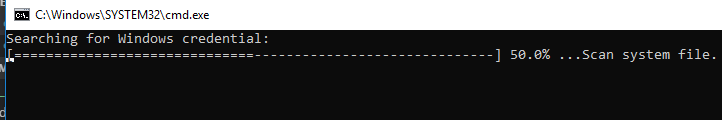
3.2 Same as <step\_2.2>, Press the red color “Start attack” button under the Back out attack section. (As shown below)



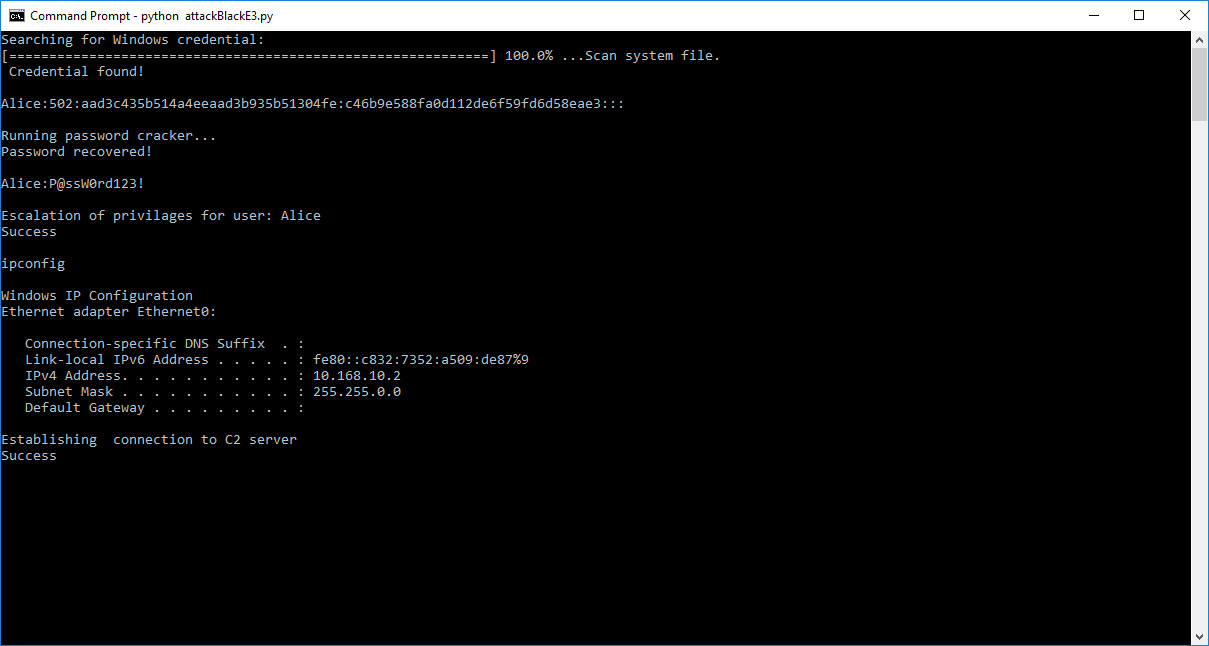
3.3 After 5 to 10 seconds, a word document named “Operation menu” will be opened automatically on the technical PC. Press the “OK” button in the edit enable pop-up window. (As shown below)



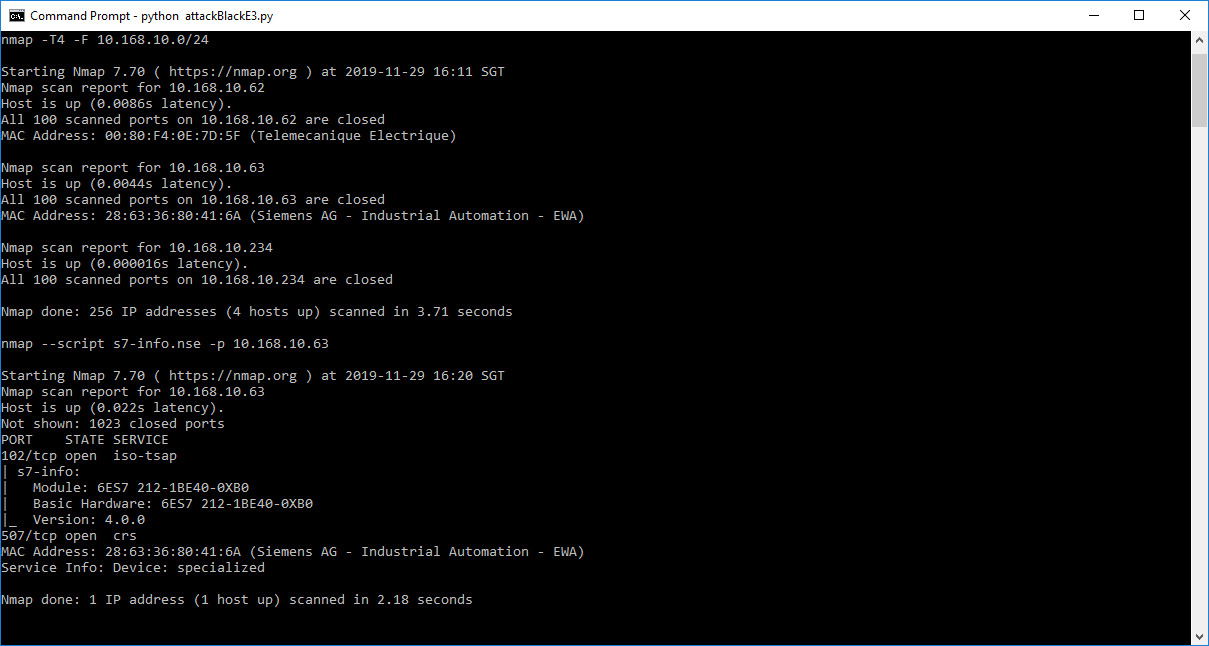
After click the Ok button, a cmd window will pop up and the attack detail information will show as below:



System information scanning result:



System attack detail information:



3.4 After the program finished running, all PLC output will be turn off. Press the HMI control button to show people the HMI cannot control the system.

3.5 Press the green color “Stop attack” button and after 20 to 30 seconds the HMI system control will recover.