Trustwave
a Singtel company

CSI OT 3D Platform Cyber Attack Demonstration

User manual

VERSION: CORPLAB-2019-T3.1-P1
31/08/2020

Prepared by
Liu Yuancheng
Senior Security Development Engineer
yuancheng.liu@trustwave.com

Wong Jun Wen
Asst R&D Manager
junwen.wong@trustwave.com

CSI OT 3D Platform Cyber Attack Demonstration User Manual

Introduction

This menu will introduce the steps to show two new cyberattack demo on the CSI OT Demo platform, namely the "False Data Injection Attack" and "Blackout Attack".

False Data Injection Attack: In this attack, we assume an additional foreign hardware (IoT/Raspberry Pi) was plug in to the OT network. This attack will manipulate the SCADA command and feedback; causes the SCADA HMI show the opposite feedback on the actual system.
This demo will attack on airport light control, where the operator will see reverse PLC feedback on the actual system, e.g. When the operator try to turn on the runway lights in the airport via HMI, the actual runway lights will be turn off.

Blackout Attack: This attack is model after 2015 Ukraine power grids cyber-attack. This attack will assume the system do not properly air-gapped, whereby the malware is enter to the system via spear phishing email. When the attack launched, all the PLC output coils (energy output) will forced to turn off.

Recommend to show "False data injection" attack first as this will not require to reset the whole OT platform via the HMI.

Steps to Show Attack Demo

Step 1 - Hardware power check

1.1 Switch ON the OT platform's power socket
1.2 Check and make sure the "Technician PC", "Orchestrator PC" and the "HMI PC" are working normally
1.2.1 Login Information (username/password):
Technical PC: admin/Qazqwerty123
HMI PC: root/Qazqwerty123
Orchestrator PC: 00000000/00000000 => orchestrator/Qazqwerty123

1.3 Check and make sure the PLC is running on correct ladder diagram and all 3 PLCs are working normally (please refer to Radiflow documentation)
1.3.1 REMEMBER to close all PLC program BEFORE proceed to next step

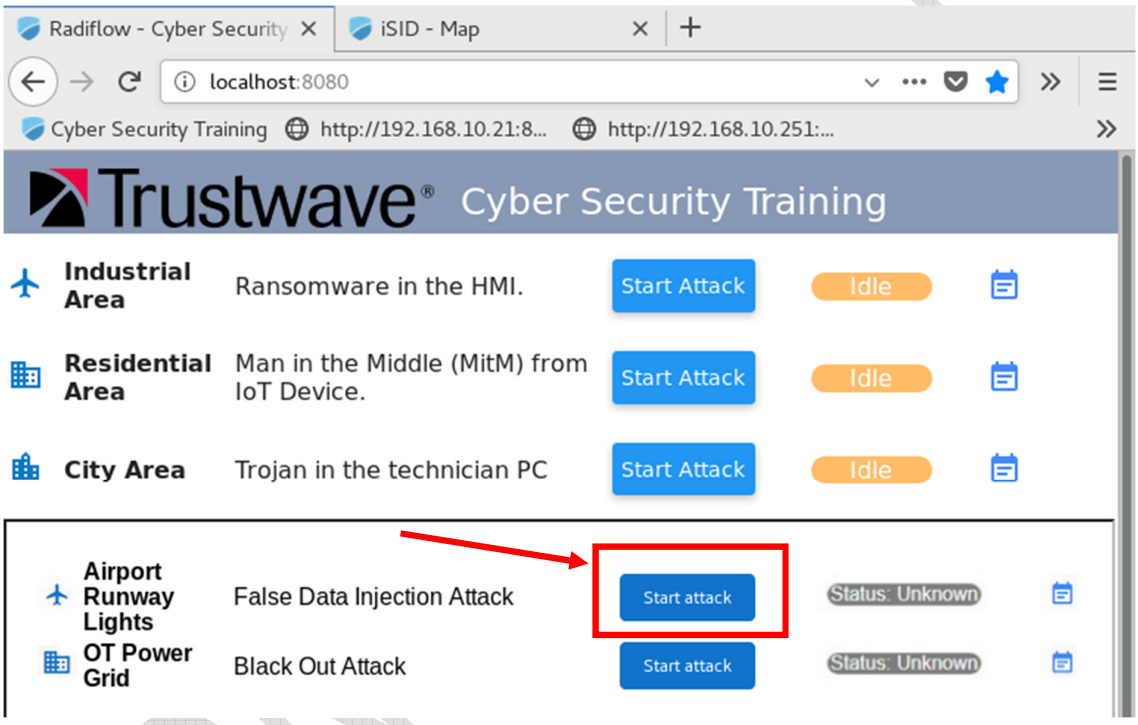
1.4 Make sure the attack Raspberry PI is power ON. (The Raspberry PI green light is on.)

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 ON state for the next step.**

2.2 Login the orchestrator PC, open web browser and type in URL: http://localhost:8080 or http://127.0.0.1:8080 and the attack control page will show as below.

2.3 To START the attack, press the 'False data injection attack' section red color "Start attack" button (marked in the red rectangle).



2.4 Wait for 10 to 20 seconds until the 'training HMI' shown the airport runway light was turn off. This indicated the false data injection attack has started successful.

2.5 Try to turn on/off the runway light from the 'training HMI' and you can see the control signal has been reversed.

2.6 To STOP the attack, press the green color "Stop attack" button, wait for 20 to 30 seconds until the runway lights is same as the state shown on the 'training HMI'. This indicate the false data injection attack has stopped successfully.

2.7 Try to turn on and off the runway light to show the HMI control has recovered.

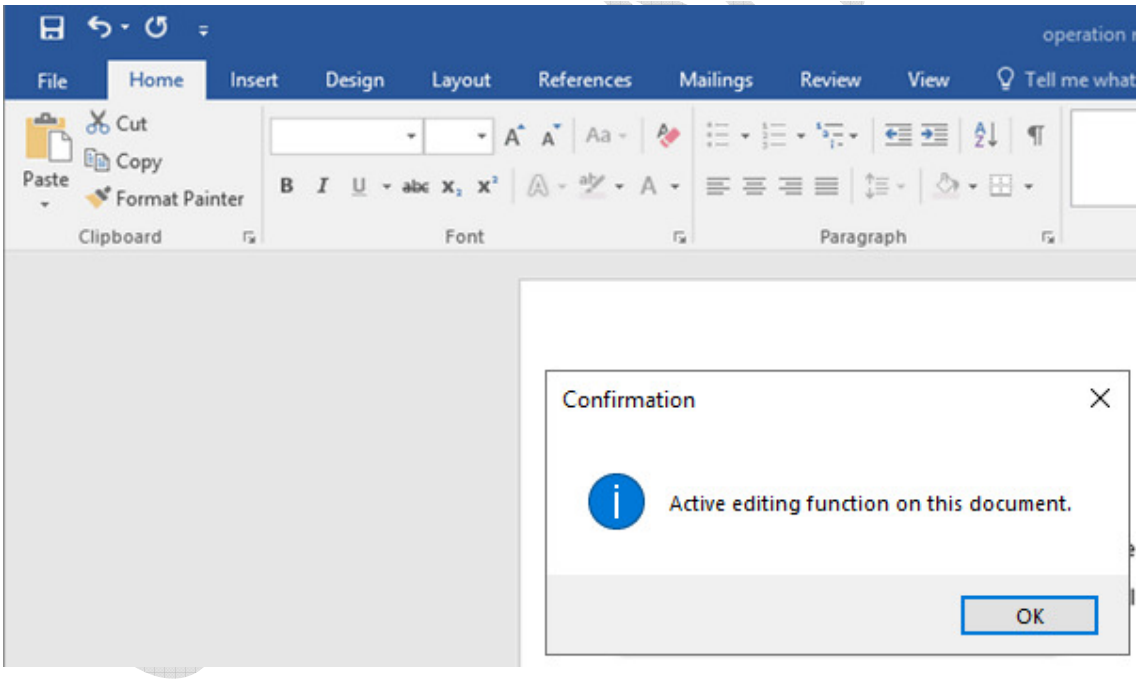
Step 3 – Show Blackout attack demo

3.1 Check and turn on all the PLC outputs via training HMI, to show the audience that the system is working normally.

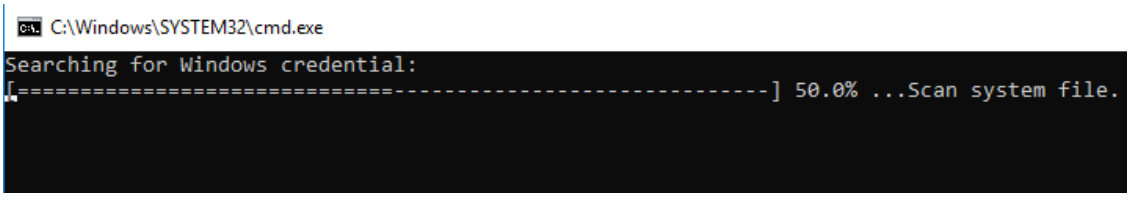
3.2 Refer to Step 2.2; press the red color "Start attack" button under the Blackout attack section to start the attack. (As shown below)

3.3 Please direct the audience attention to 'Technican PC'. After 5 to 10 seconds, a 'Microsoft Word' document named "Operation menu" will open automatically on the 'Technical PC' screen.

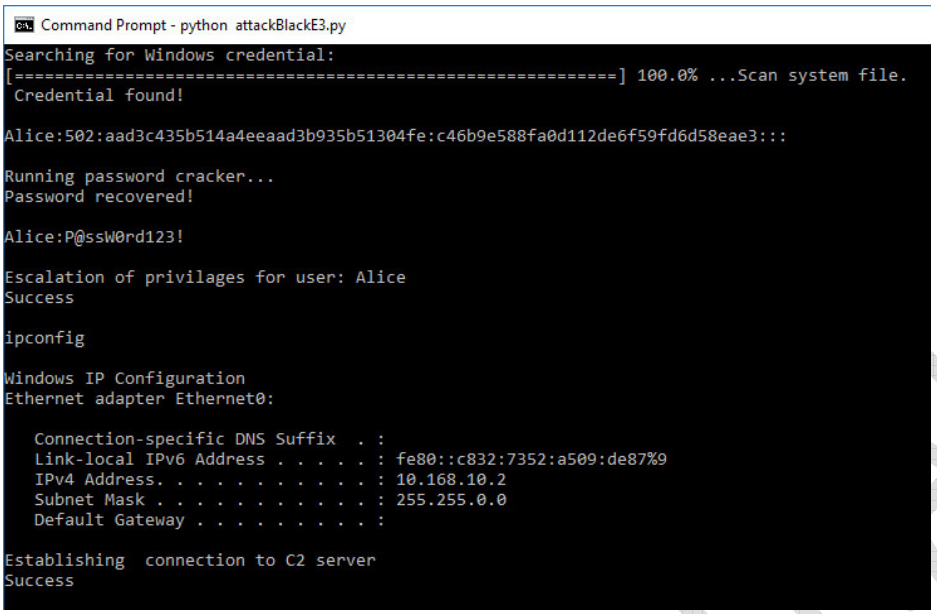
3.4 Press the "OK" button in the "Confirmation" pop-up windows. (As shown below)



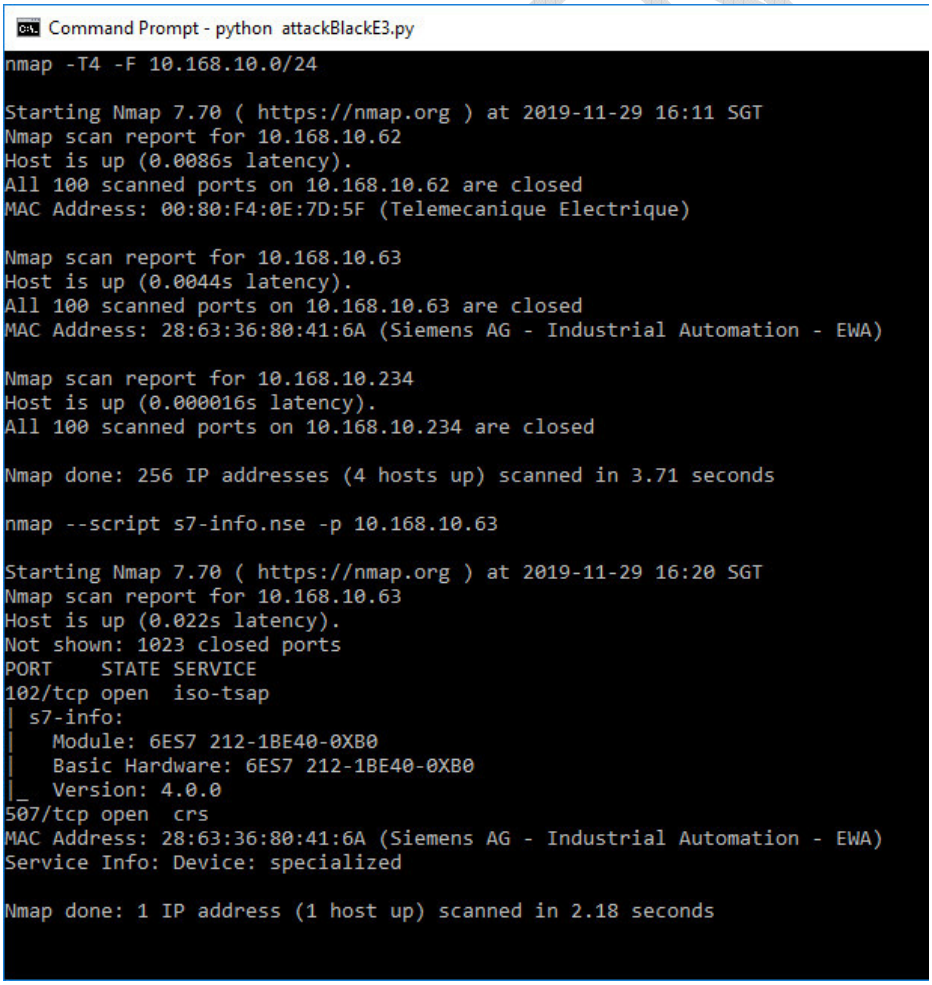
3.5 After click the 'OK' button, a 'Command Prompt Terminal' window will pop up and the attack detail information will show as below:



System information scanning result:



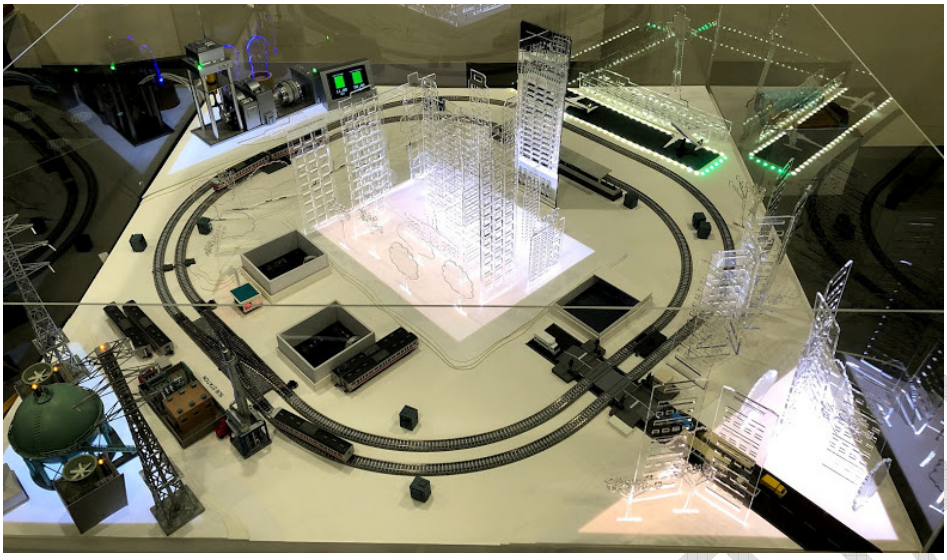
System attack detail information:

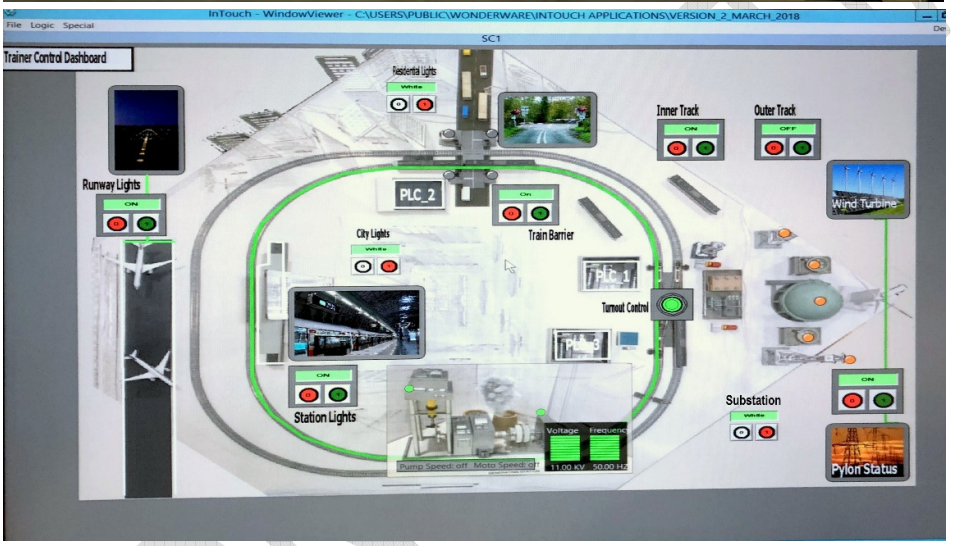


3.6 After the program finished running, all PLC output will be turn off. Try to press any of the 'Training HMI' control button to show audience that the HMI cannot control the system.

3.7 To STOP the attack, press the green color "Stop attack" button at the 'Orchestration PC'. The 'Training HMI' will normalize after 20 to 30 second.

Appendix: Default state of the OT Platform





1. Residential Lights = White
2. Substation Lights = White
3. City Lights = White
4. Pylon Status LED = ON
5. Station Lights = ON
6. Turnout Control = OFF
7. Train Barrier = ON
8. Inner Track = ON, with Trains
9. Outer Track = OFF
10. Runway Light = ON
11. Power Plant motor LED = Green
12. Power Plant pump LED = Green
13. Power Plant LCD = Green bar, Green bar, 11kV, 50 Hz
14. Power Plant siren = OFF
15. Power Plant smoke LED = ON