Title :- Ripping PLCs off, you call it pen testing, so be it !!!

Abstract: -

Todays new gen attacks and malwares have been targeting ICS systems causing huge monetary and Human life losses. The White Security community lacks knowledge and methodologies to conduct Pen-testing of PLCs. Pen-testing PLC's is very niche field which is not just requires in-depth knowledge but also there is huge dependencies in terms of the Hardware availability.
This workshop (Lab Session) will concentrate on methodologies to conduct penetration testing of real time Hardware PLCs as well as simulators to mitigates some common attacks and vulnerabilities. The workshop demonstrates basic briefing of ICS components and jargons, architecture and briefing various protocols used in ICS network, need of security and hands on session of Pen-testing of PLCs.

Draft White Paper: -

This workshop (Lab session) will intended to concentrate on methodologies to conduct penetration testing of real time Hardware PLCs as well as simulators to mitigates some common attacks, vulnerabilities and also concentrate on bridging gaps in knowledge of ICS with introducing ICS (Industrial Control System) along with briefing their jargons, typical architecture, briefing of various protocols, security concerns, tools for pen-testing and their methodologies to perform pen-test along with illustrating basic programing of PLC and their wirings.
This Lab session will put lights on those people who do not know about ICS, PLC and methodologies to pen-test PLC's. The attendees will get chance to pen-test real time Hardware PLC and simulator

In this Lab session, there are two modules i.e Module A and Module B, each modules covers different parts of workshop.

Module A : -

This module covers full theory part of PLC with introducing to ICS as follows

- Briefing of Scada : - Definition of Scada , their usage and
- examples
- Briefing of HMI : - Definition of HMI , their usage and examples

- Briefing of RTU/PLC: - Definition of RTU/PLC , their usage and
- examples
- Briefing Historian: - Definition of Historian , their usage and
- examples
- Diagram of typical Scada and plc architecture and their briefing
- Briefing of ICS protocols like Modbus,s7comm and BacNet :-
- understanding packet architecture and details of function codes
- etc.
- List of tools
- Understanding snippet of PLC program

Module B :-

This module covers Hands on session of Pen-testing with help of available tools which is mentioned in Tool Section.

- Finding PLC's on internet with Shodan and zoomeye
- Modbus Network Scanning: - This attack involves sending benign messages to all possible addresses on a Modbus network to obtain information about field devices
- Passive Reconnaissance: - This attack involves passively reading Modbus and other protocols messages or network traffic.
- Reading register values over modbus
- Reading coil values over Modbus
- Writing Register and coil values to toggle the actuators over Modbus
- Writing status of AST monitoring systems (Changing level of Diesel-petrol tank, Name of the Tank)
- Scanning and enumeration of BACnet communication.
- Toggle BMS actuators over BACnet communication.

- Reconnaissance and Enumeration of Hardware PLC (Delta and Siemens PLC, BanNet Devices) and software simulator (Modbus/TCP and Siemens s7comm).
- ON/OFF cpu of S7 PLC
- Injecting PLC programs over s7comm

- S7comm Network Scanning: - This attack involves sending benign messages to all possible addresses on a s7comm network to obtain information about field devices.
- Baseline Response Replay:- This attack involves recording genuine traffic between a master and a field device, and replaying some of the recorded messages back to the master.
- Rogue Interloper (PLC) :- This attack involves attaching a computer with the appropriate (serial or Ethernet) adap-tors to an unprotected communication link. This "man- in-the-middle" device can read, modify and fabricate Modbus messages and/or network traffic.

Tools: -

List of tools which will use in Lab session as follows

- Mbtget
- Nmap
- Plcscan
- Snmpcheck and Snmpwalk
- Arpspoof
- Metasploit auxiliary plugin for PLC
- Device – Raspberry Pi
- Modlib and pymodbus library
- Snap7 library

Hardware: -

List of hardware as follows

- Delta DVPEN01+DVP28SV plc
- Siemens s7 300 and s7 1200 plc
- SMPS
- Electric simulator board – Consist of Push buttons, PNP sensors,
- Indicators, Alarm indicators
- Raspberry Pi

Software Simulator: -

- List of simulator which will use in session as well as distribute in session
- ModbusPal :- Modbus TCP simulator
- Conpot :- Siemens s7 200 simulator. Snmp, Modbus and s7comm
- are supported protocols
- AST simulator
- OPenScada :- OpenScada is a Industrial Control Systems simulator which adds a “similar to real-world control logic” to the basic “read/write tags” feature of most PLC simulators.

Scada Application: -

- I will be using ScadaBR web application to show, how industrial scada application can affect once PLC get compromise.
- The ScadaBR is a complete supervisory system, available in Open Source license (free software). ScadaBR is used for to develop automated applications in any environment Industries,
- Laboratories, Building Automation, Sanitation, Energy Systems and more. It also supports various communication protocols including
- Modbus serials/RTU, Modbus TCP/IP, DNP3 TCP/Ip, Backnet etc.

Speaker Bio:

Arun is a Hardware, IOT and ICS Security Researcher, working with Payatu Software Labs as Sr. Security Researcher. His areas of interest are Hardware Security, SCA, Fault Injection, RF protocols and Firmware Reverse Engineering. He also has experience in performing Security Audits for both Government and private clients. He has presented a talk at the nullcon 2016,2017 Goa, GNUnify 2017, Defcamp 2017, c0c0n-x 2017, BSides Delhi 2017 and also co-trainer for Practical IOT hacking training and delivered in HITB 2017, HIP 2017, private clients in London, Australia, Sweden, Netherlands etc. He is an active member of null – The open Security community.

Rushikesh is a security analyst. Having more than six years of experience under his belt, his assignments have always been pointed towards reducing the state of insecurity for information. His research papers were accepted at NCACNS 2013, nullcon 2014, HITCON 2014, Defcamp 2014, BruCON 2015, DEFCON 24, BruCON 2016, x33fcon 2017, c0c0n-x 2017, BruCON 2017 and BSides Delhi 2017 as well he is a co-author of an intelligent evil twin tool "DECEPTICON". Being an avid CTF player, for him solace is messing up with packets, frames and shell codes.