hslatman / awesome-industrial-control-system-security

A curated list of resources related to Industrial Control System (ICS) security.

LICENSE	Initial commit	2 years ago
README.md	Merge pull request #23 from ICSrepo/patch-1	2 months ago

README.md

awesome-industrial-control-system-security

A curated list of resources related to Industrial Control System (ICS) security.

Feel free to contribute.

Tools

CSET	The Cyber Security Evaluation Tool (CSET®) assists organizations in protecting their key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.
Digital Bond's 3S CoDeSys Tools	Digital Bond created three tools for interacting with PLCs that run CoDeSys, consisting of a command shell, file transfer and NMap script.
Digital Bond's ICS Enumeration Tools	Redpoint is a Digital Bond research project to enumerate ICS applications and devices using nmap extensions. It can be used during assessments to discover ICS devices and pull information that would be helpful in secondary testing. The Redpoint tools use legitimate protocol or application commands to discover and enumerate devices and applications. There is no effort to exploit or crash anything, but be wise and careful.

GRASSMARLIN	GRASSMARLIN provides IP network situational awareness of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) networks to support network security. Passively map, and visually display, an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems.
mbtget	mbtget - Simple perl script for make some modbus transaction from the command line.
MiniCPS	MiniCPS: A toolkit for security research on Cyber-Physical Systems from Singapore University of Technology and Design (SUTD).
MODBUS Penetration Testing Framework	smod is a modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol. It is a full Modbus protocol implementation using Python and Scapy. The framework can be used to perform vulnerability assessments.
ModbusPal	ModbusPal is a MODBUS slave simulator. Its purpose is to offer an easy to use interface with the capabilities to reproduce complex and realistic MODBUS environments.
ModScan	ModScan is a new tool designed to map a SCADA MODBUS TCP based network.
NetToPLCSim	TCP/IP-Network extension for the PLC simulation software Siemens PLCSim.
Opendnp3	Opendnp3 is the de facto reference implementation of IEEE-1815 (DNP3) provided under the Apache License.
PLCinject	PLCinject can be used to inject code into PLCs.
plcscan	Tool for scaning PLC devices over the s7comm or modbus protocol.
Quickdraw IDS	The Quickdraw IDS project by Digital Bond includes Snort rules for SCADA devices and so-called preprocessors for network traffic. The preprocessors provide significant additional value because of their ability to reconstruct the protocol and state for use by Snort.
SCADAShutdownTool	SCADAShutdownTool is an industrial control system automation and testing tool allows security

	researchers and experts to test SCADA security systems, enumerate slave controllers, read controller's registers values and rewrite registers data.
Snap7	Snap7 is an open source, 32/64 bit, multi-platform Ethernet communication suite for interfacing natively with Siemens S7 PLCs. The new CPUs 1200/1500, the old S7200, the small LOGO 0BA7/0BA8 and SINAMICS Drives are also partially supported.
S7 Password Bruteforcer	A tool to bruteforce the password used by S7 instances from a PCAP using a dictionary. Original created by SCADAStrangelove.
splonebox	splonebox is an open source network assessment tool with focus on modularity. It offers an ongoing analysis of a network and its devices. One major design decision features development of custom plugins, including ones for industrial communication protocols.
Wireshark	Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. It has support for many protocols used in ICS.

Distributions

Moki Linux	Moki is a modification of Kali to encorporate various ICS/SCADA Tools scattered around the internet, to create a customized Kali Linux geared towards ICS/SCADA pentesting professionals.
SamuraiSTFU	SamuraiSTFU takes the best in breed security tools for traditional network and web penetration testing, adds specialized tools for embedded and RF testing, and mixes in a healthy dose of energy sector context, documentation, and sample files, including emulators for SCADA, Smart Meters, and other types of energy sector systems to provide leverage a full test lab.

Honeypots

Conpot	Conpot is a low interactive server side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. It features easy customization and and behaviour mimicking, amongst others, and can be extended with real HMIs. Built and maintained under the Honeynet project.
GasPot	GasPot is a honeypot that has been designed to simulate a Veeder Root Gaurdian AST. These Tank Gauges are common in the oil and gas industry for Gas Station tanks to help with Inventory of fuels. GasPot was designed to randomize as much as possible so no two instances look exactly the same.
T-Pot	T-Pot is a combination of several honeypots that run in docker containers. Suricata and the ELK stack are used for security monitoring and visualization. Amongst others, it features Conpot and eMobility, which are an ICS and next generation transport infrastructure honeypots.

Data

4SICS ICS Lab PCAPS	The "Geek Lounge" at 4SICS contains an ICS lab with PLCs, RTUs, servers, industrial network equipment (switches, firewalls, etc). These devices are available for hands-on "testing" by 4SICS attendees and traffic has been captured from these.
DEF CON 23 ICS Village PCAPS	PCAPS from the 23rd DEF CON.
ICS Map	A map created from data gathered by Shodan showing ICS devices. Data is made available for further analysis.
ICS Radar	Data gathered from several types of ICS protocols by Shodan visualized on a globe.
S4x15 ICS Village	PCAPS from the S4x15 CTF as used during the contest.
S7 PCAP samples	Sample files for Wireshark S7 protocol dissector plugin.

SCADAPASS	The famous SCADA StrangeLove Default/Hardcoded Passwords List.
TRISIS/TRITON/HATMAN malware repository	Repository containting original and decompiled files of TRISIS/TRITON/HATMAN malware targeting Triconex Safety Instrumented System (SIS) controllers.

Feeds and News

ICS-CERT Alerts	The ICS-CERT Alert feed is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.
ICS-CERT RSS Feed	The RSS feed by the United States ICS-CERT lists news and newly released vulnerability advisories.
Industrial Security Alerts	Siemens provides alerts for its industrial systems via this page and RSS feed.
North American Electric Reliability Corporation (NERC) Alerts	NERC provides alerts for Bulk Electric System (BES) security advisories and industry recommendations.
ABB Cybersecurity Alerts and Notifications	ABB provides alerts for its cyber security incidents and software vulnerabilities.
Schneider Electric Cybersecurity Alerts and Notifications	Get the latest updates and alerts on Cyber Security and Compliance from Schneider Electric Software.

Conferences and Conference Material

CS3STHLM	the Stockholm international summit on Cyber Security in SCADA and Industrial Control Systems - is an annual summit that gather the most important stakeholders across critical processes and industries. CS3STHLM has been organized since 2014, and has quickly become the premier ICS Security Summit in Northern Europe.
CS4CA	Cyber Security for Critical Assets is a global series of summits focusing on cyber security for critical infrastructure.
SANS ICS Summit Archives	Central repository for the presentation material for the SANS ICS Summits held worldwide.
SANS ICS Cybersecurity Conference (WeissCon)	Affectionately known as WeissCon after it's founder Joe Weiss, the conference is now owned and operated by SecurityWeek and usually runs in October at different locations each year in the US.

Literature

Library of Resources for Industrial Control System Cyber Security	SCADAhacker.com's ultimate list of ICS/SCADA cybersecurity resources.
Applied Cyber Security and the Smart Grid	Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure by Eric D. Knapp and Raj Samani.
A Collection of Resources for Getting Started in ICS/SCADA Cybersecurity	Robert M. Lee's thoughts on some good resources on ICS & SCADA security.

Hacker Machine Interface - The State of SCADA HMI Vulnerabilities	A TrendLabs Research Paper from the Trend Micro Zero Day Initiative Team about the current state of SCADA and HMI security.
Handbook of SCADA/Control Systems Security	This comprehensive handbook covers fundamental security concepts, methodologies, and relevant information pertaining to supervisory control and data acquisition (SCADA) and other industrial control systems used in utility and industrial facilities worldwide.
SCADA Cybersecurity Framework	Paper describing what a SCADA Cyber Security framework should consist of.
Industrial Network Security, Second Edition	Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by Eric D. Knapp and Joel Thomas Langill.
Power System SCADA and Smart Grids	The book brings together in one concise volume the fundamentals and possible application functions of power system supervisory control and data acquisition (SCADA). Not security-oriented and geared towards power systems, but a good primer into SCADA nonetheless.
NIST SP 800-82, Revision 2	Guide to Industrial Control Systems (ICS) Security by NIST.
The Industrial Control System Cyber Kill Chain	This SANS paper describes the ICS Cyber Kill Chain. It tailors the Lockheed Martin Kill Chain to typical, two phase attacks on ICS systems.
An Abbreviated History of Automation, Industrial Control Systems, and Cybersecurity	This SANS paper looks at the background on ICS cybersecurity. Well worth the read to make sure you understand many of the events that have occurred over the past twenty years and how they've inspired security in ICS today.
Control Engineering -	Control Engineering magazine's cybersecurity news and literature.

Networking and Security - CyberSecurity	

Introduction to ICS, SCADA, & PLCs

PLC Training Org	Site organizes all essential topics related to PLC training up to SCADA systems. While security is interwoven within the 10 learning phases, this is a great security article on the site for those just starting out.
Control System Basics	YouTube video explaining control system basics including the type of logic these systems use to sense and create physical changes to take action upon.
SCADA Systems - Utility 101 Session with Rusty Wiliiams	Utility industry professional Rusty Williams explains SCADA from an electric utility perspective.
Control System Lectures	Brian Douglas YouTube video series where he covers a wide range of topics on control systems in a very easy to process way.
The PLC Professor	The PLC Professor and his website plcprofessor.com contains a lot of great resources for learning what programmable logic controllers (PLCs) and other types of control systems and their logic are and how they work.
Serial Communications RS232 and RS485	John Rinaldi of Real Time Automation describes Serial communications RS232 and RS485.
All You Need To Know About MODBUS-RTU	John Rinaldi of Real Time Automation describes MODBUS-RTU.

MODBUS Data Structures	John Rinaldi of Real Time Automation describes MODBUS data structures.
All You Need to Know About MODBUS-TCP	John Rinaldi of Real Time Automation describes MODBUS-TCP.
How Ethernet TCP/IP is Used by Industrial Protocols	John Rinaldi of Real Time Automation describes Ethernet TCP/IP.

License