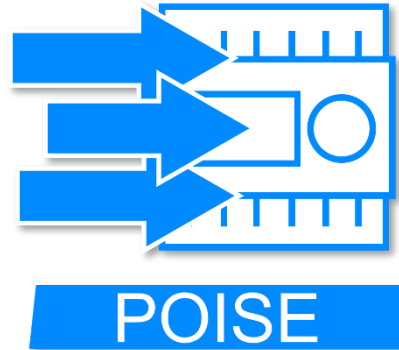


PRACTICAL OFFENSIVE INDUSTRIAL SECURITY ESSENTIALS STUDY ROADMAP



WEEK 1	Evolution of Industrial Devices and Communication, Contrasting IT and OT	Attack Surfaces and Common Security Challenges	Offensive OSINT and Exposed Industrial Devices	Setting Up the Lab Environment	Setting Up the Lab Environment	Introduction to Kali Linux and Pentesting Tools	Introduction to Kali Linux and Pentesting Tools
WEEK 2	Programmable Logic Controllers and Siemens Simatic S7 Controllers	Profinet/S7Comm Protocol Stack and Wireshark Exercise	OSINT for Exposed S7 Controllers	Common Pentest Tools for S7 Controllers	Common Pentest Tools for S7 Controllers	Review and Summarizing S7 Controller Learnings	Penetration Testing S7 Controller
WEEK 3	Penetration Testing S7 Controller	Penetration Testing S7 Controller, Findings and Mitigations	Summarizing Penetration Testing Learnings	Smart Factories, Industrial MQTT and Edge Gateways	IIOT Communication with MQTT, Protocol Stack and Wireshark Exercise	OSINT for Exposed MQTT Services	Common Pentest Tools for MQTT

PRACTICAL OFFENSIVE INDUSTRIAL SECURITY ESSENTIALS STUDY ROADMAP

WEEK 4	Review and Summarizing IloT/MQTT Learnings	Penetration Testing IloT/MQTT	Penetration Testing IloT/MQTT, Findings and Mitigations	Summarizing Penetration Testing Learnings	EnIP/CIP based Devices and Rockwell LOGIX5561 Controller	EtherNet/IP/ Common Industrial Protocol Stack and Wireshark Exercise	EtherNet/IP/ Common Industrial Protocol Stack and Wireshark Exercise
WEEK 5	Common Pentest Tools for EnIP/CIP based Devices	OSINT for Exposed EnIP/CIP Devices	Review and Summarizing EnIP/CIP based Device Learnings	Penetration Testing EnIP/CIP Devices	Penetration Testing EnIP/CIP Devices, Findings and Mitigations	Summarizing Penetration Testing Learnings	Fuel Station Infrastructure and Automated Tank Gauges (ATG)
WEEK 6	Configuring the TLS-350 via Function Codes	Common Pentest Tools for ATGs	OSINT for Exposed ATG Devices	OSINT for Exposed ATG Devices	Review and Summarizing ATG Learnings	Penetration Testing ATGs	Penetration Testing ATGs, Findings and Mitigations
WEEK 7	Summarizing Penetration Testing Learnings	Human Machine Interfaces (HMI) for Process Control	Siemens KTP HMI Hardware	HMI Screen Design and Remote Access	Common Pentest Tools for HMIs and Remote Access	Common Pentest Tools for HMI Remote Access	OSINT for Exposed HMIs
WEEK 8	Review and Summarizing HMI Learnings	Penetration Testing HMIs	Penetration Testing HMI, Findings and Mitigations	Summarizing Penetration Testing Learnings	Modicon Industrial Controllers, Modbus TCP Protocol	Modbus TCP Protocol Stack and Wireshark Exercise	Memory Addressing in Modbus Controllers

PRACTICAL OFFENSIVE INDUSTRIAL SECURITY ESSENTIALS STUDY ROADMAP

WEEK 9	Common Pentest Tools for Modbus Devices	Review and Summarizing Modbus Device Learnings	Penetration Testing Modbus Devices	Penetration Testing Modbus Devices, Findings and Mitigation	Infrastructure Substation and IEC-104 Communication	IEC-104 Protocol Stack and Wireshark Exercise	Common Pentest Tools for IEC-104 Protocol
WEEK 10	Review and Summarizing IEC-104 Learnings	Penetration Testing IEC-104, Findings & Mitigation, Summarizing Pentest Learnings	Historically Evolved Shop Floors, OT Networks, and VPN Access	Scanning a Legacy OT Network	Understanding Common Security Challenges	Risk of Flat OT Networks and Internet Access Gateways	Adversary Maturity Levels in IEC/ISA 62443
WEEK 11	Threat Modelling with Mitre ICS ATT&CK	Threat Modelling with Mitre ICS ATT&CK	Mitigation and Protection with Defense in Depth	Mitigation and Protection with Defense in Depth	System Hardening of PLCs	System Hardening of HMIs	Secure OT Network Design with Segmentation and DMZ
WEEK 12	Secure OT Network Design with Segmentation and DMZ	Securing Remote Access Services	Recap of Penetration Testing Exercises	Recap of Penetration Testing Exercises	Recap of Common Security Challenges	Recap of Defense in Depth	Recap of Defense in Depth