Man-In-The-Middle Attack Against Modbus TCP Illustrated with Wireshark

By Created by:Gabriel Sanchez

Download File

Man-In-The-Middle Attack Against Modbus TCP Illustrated with Wireshark (PDF, 3.46MB)Published: 20 Oct, 2017

Though attacks on the industrial control system (ICS) and their protocols are not a new occurrence, recent years have highlighted a growing trend in such attacks. To make matters worse, cyber defenders have also dealt with a slow migration to more secure ICS protocols due to costs associated with equipment downtime. With the increase in attacks and the slow migration to more secure ICS protocols, it is crucial for cyber defenders to be able to quickly set up labs to mimic and observe how potential attacks on the ICS network function so that necessary defenses and detection mechanisms can be put in place. This paper lays out how to setup a lab with multiple virtual machines and ICS software that can observe a Master workstation controlling a PLC. First, Wireshark will be used to illustrate and compare normal Modbus TCP communications between the Master and PLC workstations. Wireshark will then be used to demonstrate and compare a MITM attack with an Ettercap filter that manipulates the Modbus TCP communications against both workstations.

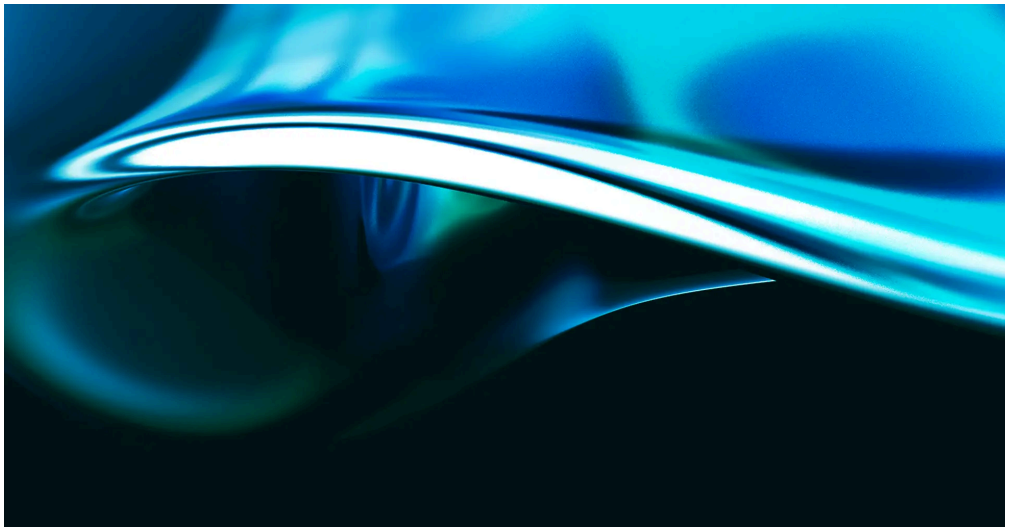
Additional resources

Related courses

- Slide 1 of 7

  ICS515: ICS Visibility, Detection, and Response

  ICS515Industrial Control Systems Security



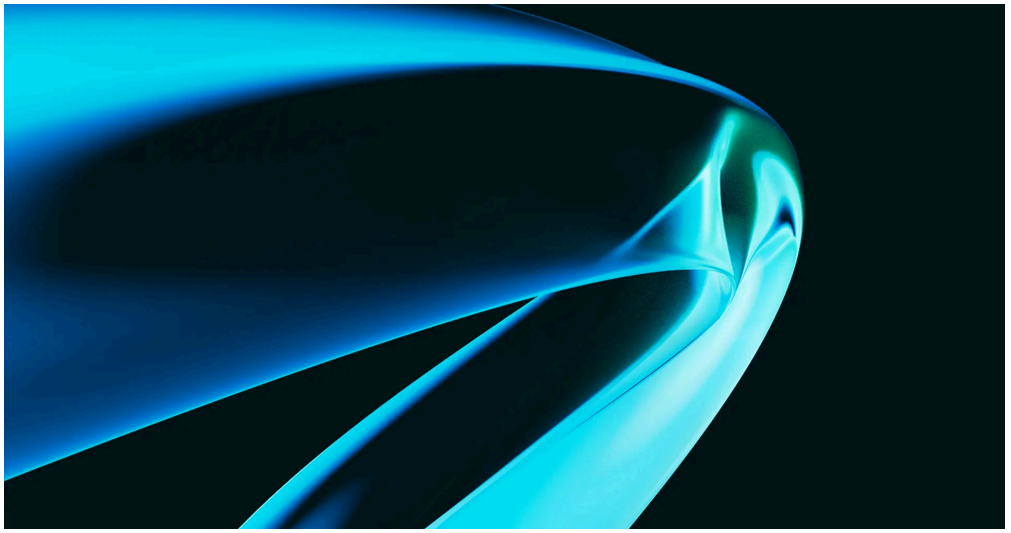
- GIAC Response and Industrial Defense (GRID)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 22 Hands-On Labs

View course detailsRegister

- Slide 2 of 7

ICS418: ICS Security Essentials for Leaders

ICS418Industrial Control Systems Security



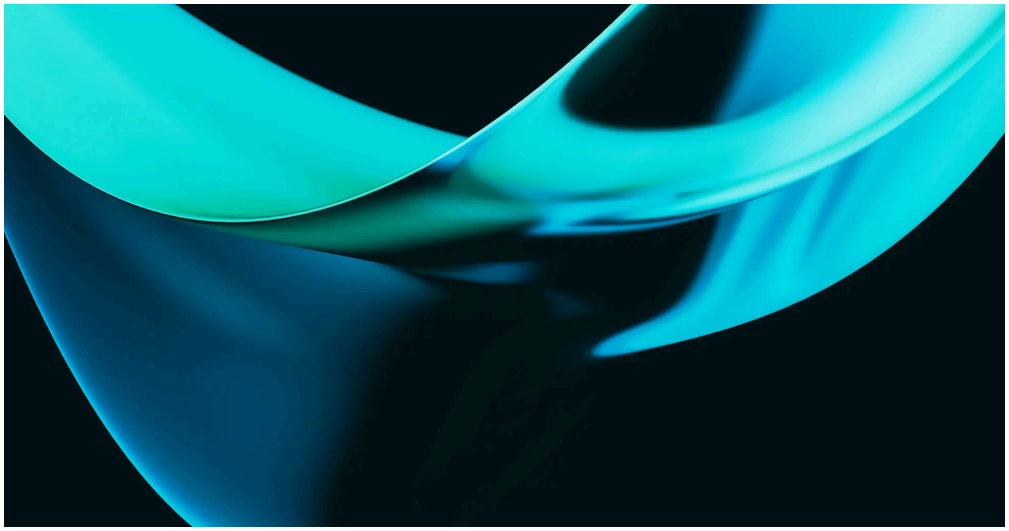
- 12 CPEs / 12 Hours (Self-Paced)
- Labs: 12 Hands-On Labs

View course detailsRegister

- Slide 3 of 7

ICS613: ICS/OT Penetration Testing & Assessments

ICS613Industrial Control Systems Security



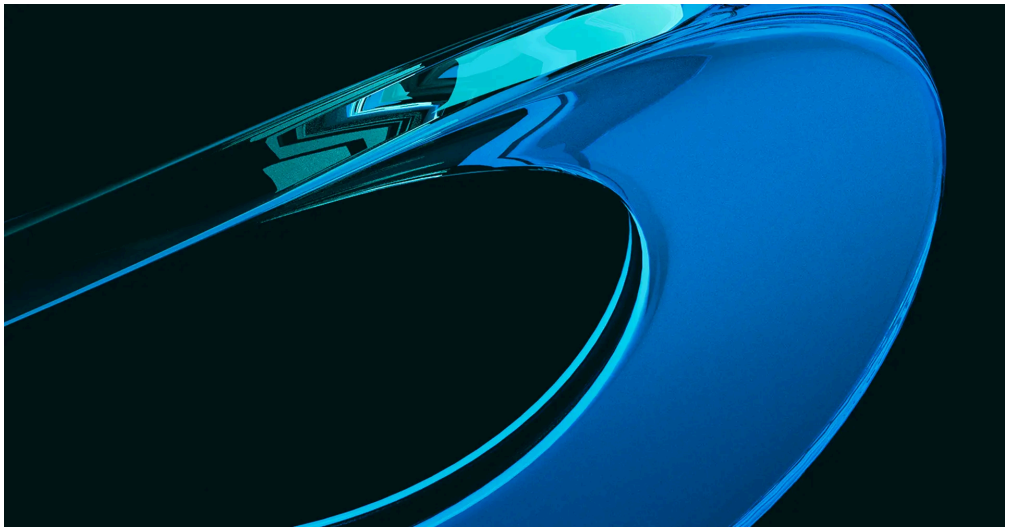
- 5 Days (Instructor-Led)
- 30 CPEs / 30 Hours
- Labs: 27 Hands-On Labs

View course detailsRegister

- Slide 4 of 7

ICS456: Essentials for NERC Critical Infrastructure Protection

ICS456Industrial Control Systems Security



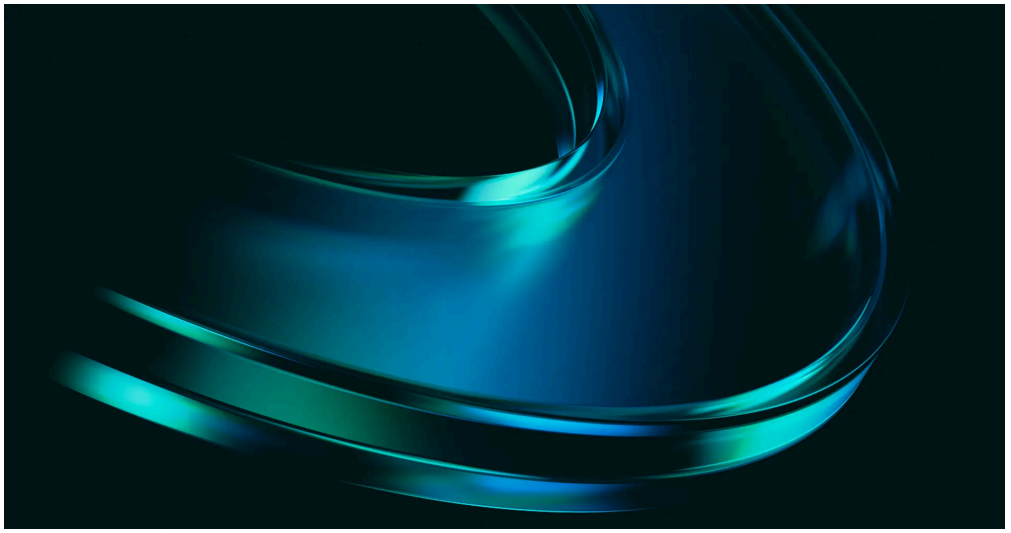
- GIAC Critical Infrastructure Protection (GCIP)
- 5 Days (Instructor-Led)
- 31 CPEs / 31 Hours (Self-Paced)
- Labs: 23 Hands-On Labs

View course detailsRegister

- Slide 5 of 7

ICS310: ICS Cybersecurity Foundations

ICS310Industrial Control Systems Security



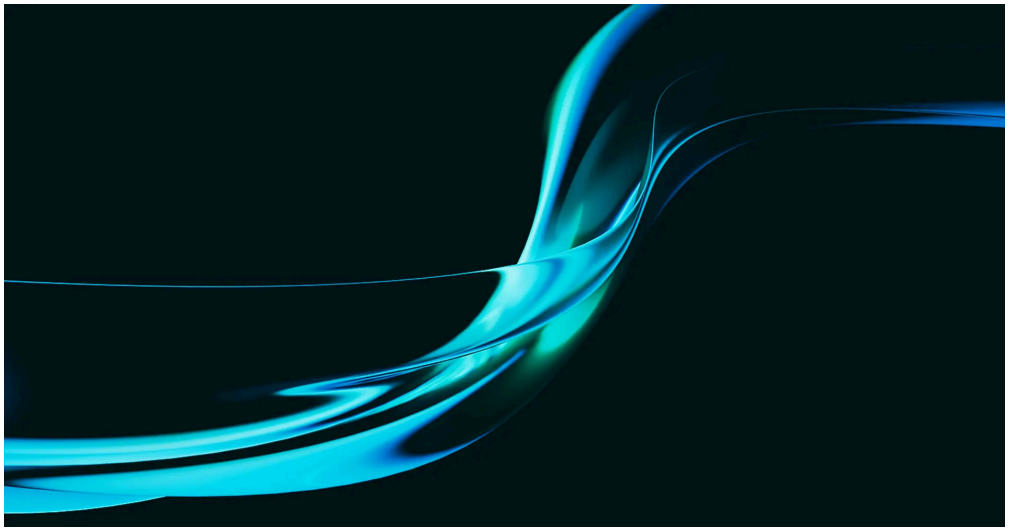
- 12 CPEs / 12 Hours (Self-Paced)
- Labs: 3 Hands-On Labs

View course detailsRegister

- Slide 6 of 7

ICS410: ICS/SCADA Security Essentials

ICS410Industrial Control Systems Security



- GIAC Global Industrial Cyber Security Professional (GICSP)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 15 Hands-On Labs

View course detailsRegister

- Slide 7 of 7

ICS612: ICS Cybersecurity In-Depth

ICS612Industrial Control Systems Security

- 5 Days (Instructor-Led)
- 30 CPEs / 30 Hours
- Labs: 31 Hands-On Labs

View course detailsRegister
