



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

Pentesting a Sistemas SCADA ICS (OT)

MSc. Ing. Ibar Mario Vásquez Ramos

Especialista en Seguridad de la información

2022

root@localhost# whoami



MSc. Ing. Ibar Mario Vásquez Ramos
Especialista en Seguridad de la información

- **Maestría MBA España en la Escuela Europea de Negocios.**
- **Maestría en informática forense, auditoría de sistemas y seguridad de la información UMSA.**
- **Maestría en gestión y administración educativa UPEA.**
- **ISO 27001 Lead Implementer**
- **ISO 31000 Risk Manager**
- **CEH, CPENT, CCNA, DBA, MTCNA, MTCUME, MTCRE, MTCINE.**



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMÁTICA**
28 a 30 de Noviembre • La Paz, Bolivia

Contenido de la ponencia

Constará de 2 partes (teórica, práctica):

1. Introducción
2. Algo de Conceptos y Definiciones:
 - IT VS OT
 - SCADA (planta nuclear, MTU)
 - ICS
1. ¿Por qué me causó curiosidad?
 - a. Noticias... Guerra Rusia Ucrania
2. Laboratorio práctico
 - Pentesting ICS/SCADA



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMATICA**
28 - 30 de Noviembre - La Coruña



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

01

INTRODUCCIÓN

Pentesting a Sistemas SCADA
ICS (OT)

Introducción



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMATICA**
28 - 30 de Noviembre - La Paz, Bolivia

- Hoy las redes ICS SCADA son totalmente críticas para cualquier país, ya que ellas controlan termonucleares, centrifugadoras, tanques de lubricantes en petroleras, tanques de presión y otros.





4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

02

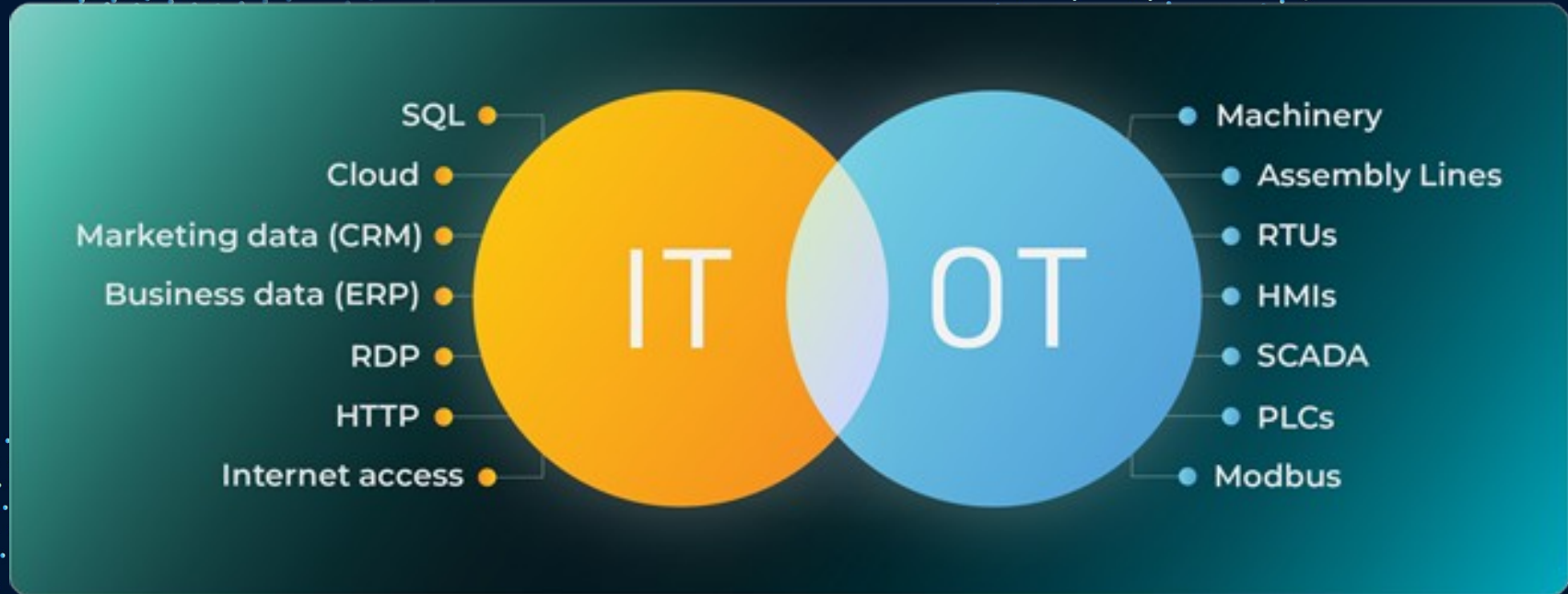
CONCEPTOS

Pentesting a Sistemas SCADA
ICS (OT)

IT VS OT



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMATICA**
20 y 30 de Noviembre - La Paz, Bolivia



SCADA



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

S C A D A

Acrónimo de:

Supervisory Control And Data Acquisition

Control y Supervisión de Adquisición de Datos

- TRANSPORTE DE PETRÓLEO (TUBERÍAS)
- TRANSPORTE DE GAS EN (GASODUCTOS)
- PLANTAS DE ENERGÍA
- FERROCARRILES
- TRÁFICO AÉREO (sensores en aeropuertos)
- INDUSTRIAS ALIMENTICIAS
- HOSPITALES
- FÁBRICAS
- OTROS

Operational Technology OT

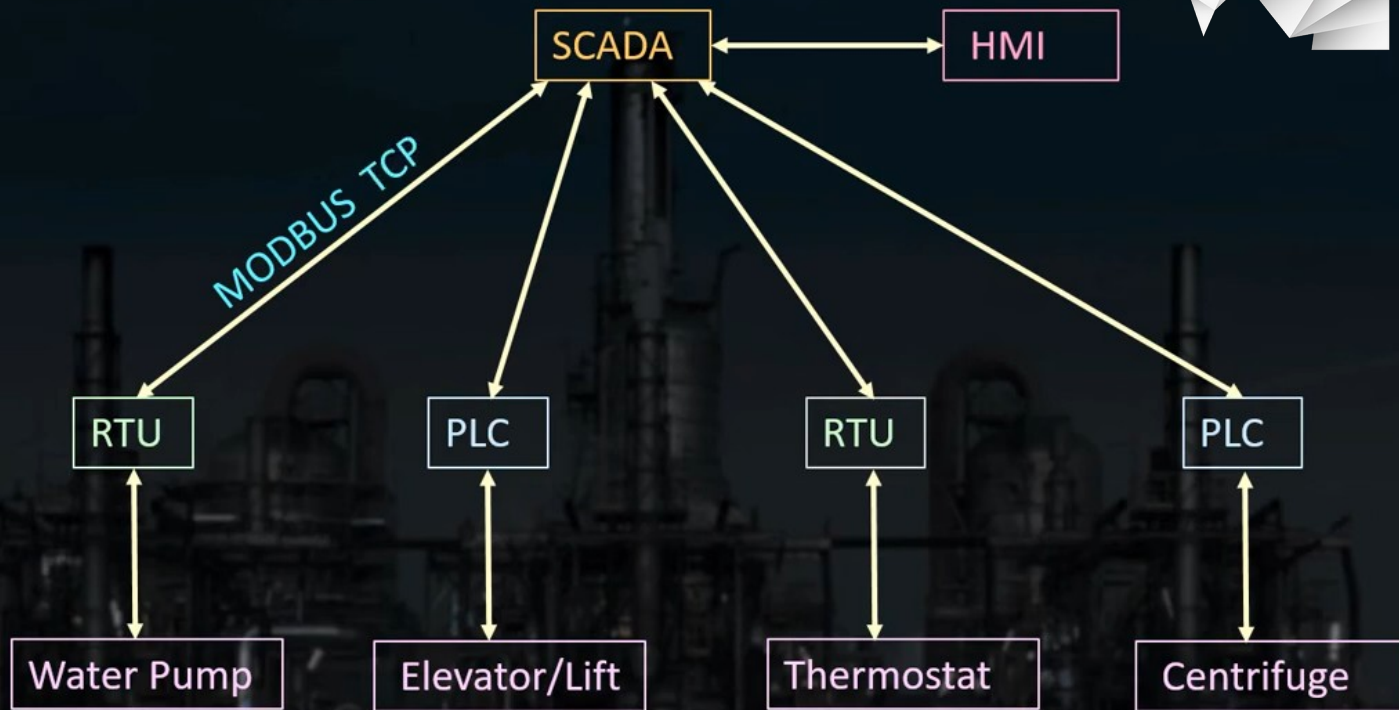


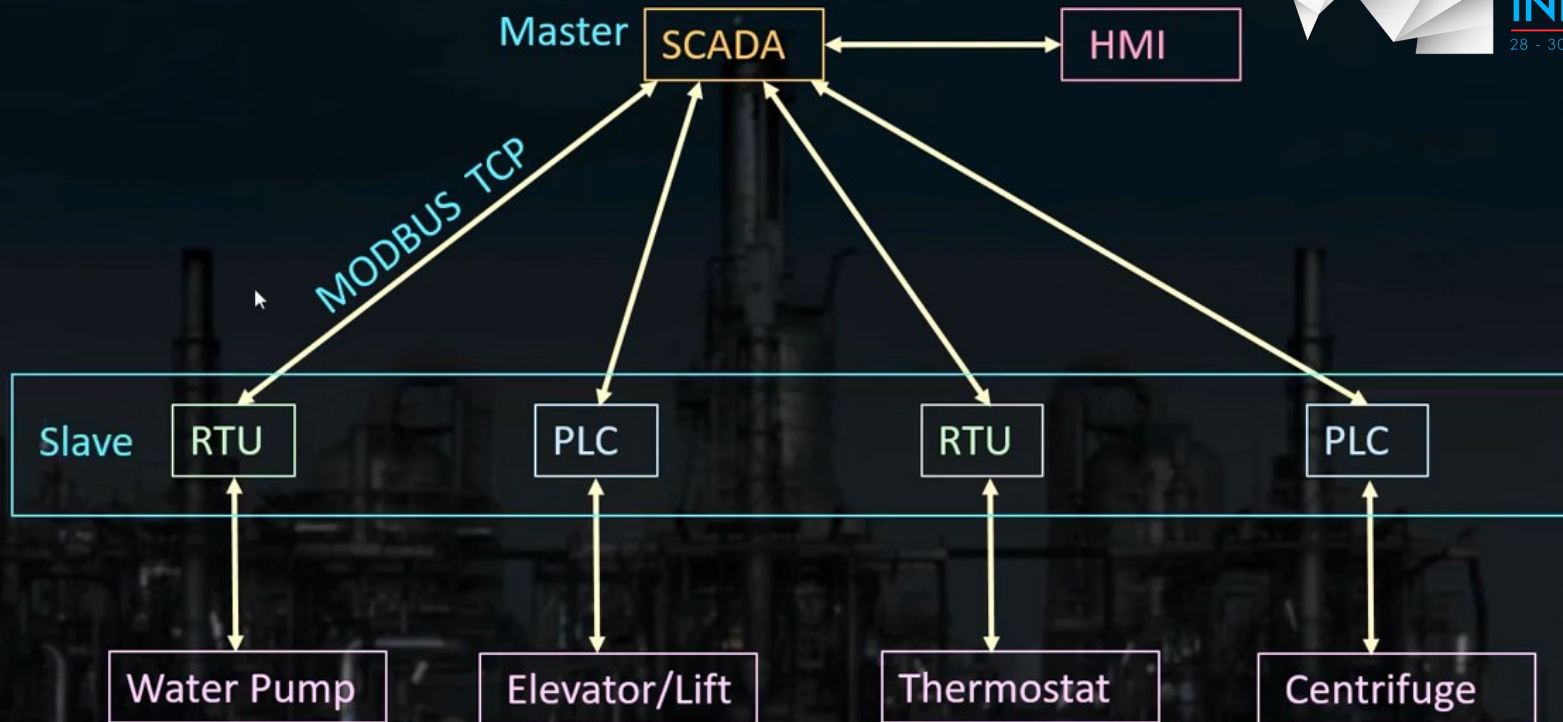
4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMÁTICA**
28 - 30 de Noviembre - La Paz, Bolivia

- **Hardware y Software que monitorea y controla dispositivos físicos en las industrias.**

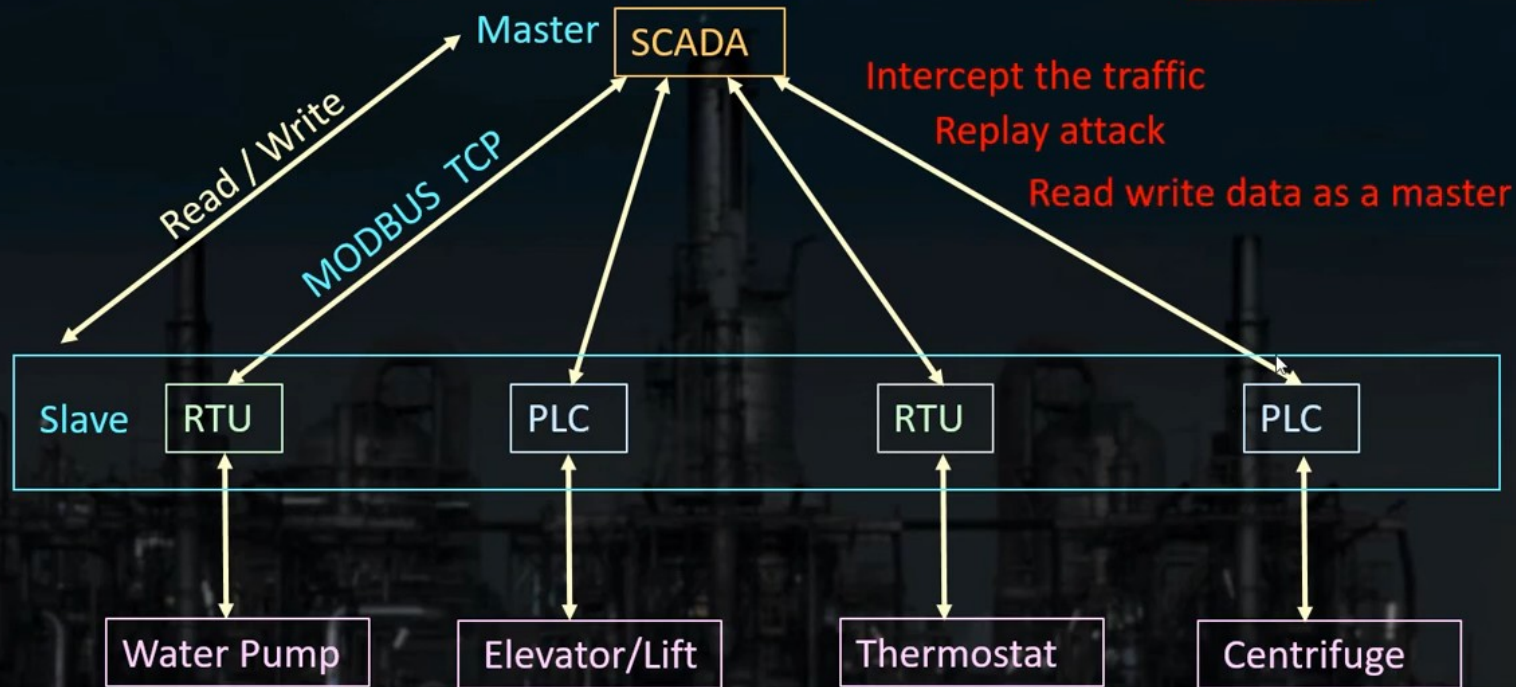
ICS - Industrial Control Systems

- **Dispositivos, programas y redes que administran equipos industriales y los procesos de su infraestructura.**



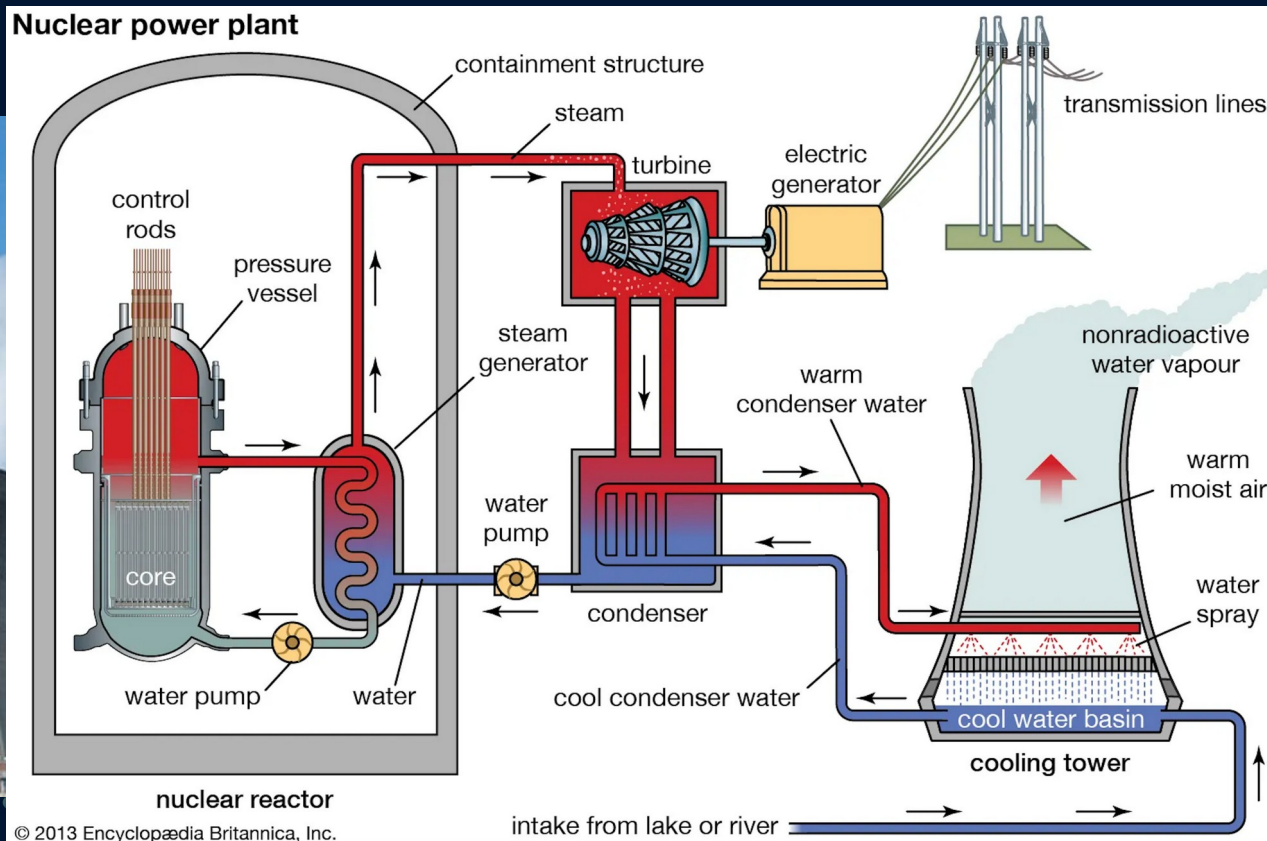


Attacker





¿Y en una planta nuclear?



¿Qué es un MTU?



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMÁTICA**
28 - 30 de Noviembre - La Paz, Bolivia

**Master
Terminal
Unit**





4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

03

¿Por qué me causó curiosidad?

Pentesting a Sistemas SCADA
ICS (OT)

Noticias...



RTVE Noticias ✓

1.44 M de suscriptores



4TO. CONGRESO INTERNACIONAL

SEGURIDAD INFORMÁTICA

28 - 30 de Noviembre - La Paz, Bolivia

rtve
Noticias

UCRANIA RECLUTA HACKERS

A LO QUE VINIMOS!



4TO. CONGRESO INTERNACIONAL
**SEGURIDAD
INFORMÁTICA**
2009, Noviembre - La Paz, Bolivia





4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

04

Pentesting ICS/SCADA

Pentesting a Sistemas SCADA
ICS (OT)



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

04

Pentesting ICS/SCADA

Pentesting a Sistemas SCADA
ICS (OT)



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

04

Pentesting ICS/SCADA

Pentesting a Sistemas SCADA
ICS (OT)



4TO. CONGRESO INTERNACIONAL

**SEGURIDAD
INFORMÁTICA**

28 - 30 de Noviembre - La Paz, Bolivia

Gracias!

@ibarmario

**A PICTURE
IS WORTH A
THOUSAND
WORDS**





A PICTURE REINFORCES THE CONCEPT

Images reveal large amounts of data, so remember: use an image instead of long texts