Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Attacking ICS Plant #1 – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Attacking ICS Plant #1 – Daniel Cruz Santana |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/10/2025 |
| **Link** | https://tryhackme.com/room/attackingics1 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Daniel Cruz Santana | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/09/2025 | Produção |
| **1** | 02/10/2025 | Revisão |
| **2** | 02/10/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | OT/ICS, SCADA, Modbus protocol |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[**Contextualização 3**](#_tyf4j5gnbsaw)

[**Desenvolvimento 3**](#_bhfrd6gd9ujj)

[Which is the function used to read holding registers in pymodbus library? 3](#_u9ug1qvwt1g2)

[Which is the function used to write holding registers in the pymodbus library? 4](#_xi0qqe3gaokl)

[How many phases can we observe? 4](#_g5dqmxq3kgne)

[How many sensors can we observe? 5](#_yvbp0dmnljki)

[How many actuators can we observe? 5](#_s60wop85k37u)

[Using the script discovery.py, how many registers can we count? 6](#_16kqfleo5w1q)

[After the plant is started and a bottle is loaded, how many registers are continuously changing their values? 6](#_p2aqylj270mb)

[Which is the minimum observed value? 6](#_3lm38ml33t5z)

[Which is the maximum observed value? 6](#_eqs7ghu2rumi)

[Which registry is holding its value? 6](#_wzg2yhr8s9lh)

[Which registries are set to 1 while the nozzle is filling a bottle? 6](#_n32hffc8h7x7)

[Which registries are set to 1 while the roller is moving the bottles? 7](#_nit5tqk9sdnh)

[Which is the color of the water level sensor? 7](#_fgjw7zgje2p1)

[Which is the color of the bottle sensor? 7](#_gkki4mqcdbzf)

[If you observe the plant at the very beginning, which is the registry associated with the roller? 8](#_pyk0ang126pw)

[Based on the previous answer, which is the registry associated with the water level sensor? 8](#_za8hxrl235ke)

[Which is the registry associated with the nozzle? 8](#_nuiksp298bth)

[Shutdown the plant and avoid the plant manager starts it again. 8](#_dz0fdq4ec4ng)

[Start the plant, open the nozzle while bottles are moving. 9](#_bnpdbwew6fpj)

[Start the plant, open the nozzle and stop the roller. 9](#_227s9ngq9ltt)

[Repeat attack in question 1 abusing sensor registries. 10](#_8wt96nux5cng)

[Repeat attack in question 2 abusing sensor registries. 10](#_k5xpkldpcluj)

[Repeat attack in question 3 abusing sensor registries. 10](#_rgjro9ojsuum)

[**Conclusão 11**](#_556asxnnmrqg)

[**Referências 11**](#_sqai22ovdnf5)

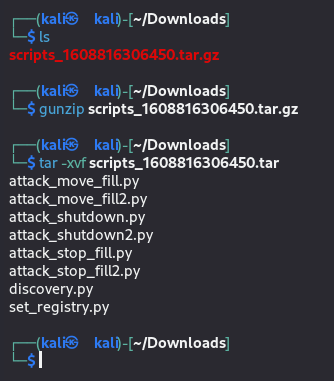
# Contextualização

Esse CTF fornece uma breve introdução sobre Operacional Technology (OT), Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) e protocolo ModBus. A parte prática aborda com maior destaque um ICS, com foco no protocolo Modbus, através da simulação de uma planta industrial.

# Desenvolvimento

## Which is the function used to read holding registers in pymodbus library?

Para responder a essa e todas as outras perguntas, é preciso baixar os arquivos disponibilizados, descompactá-los e desagrupá-los:

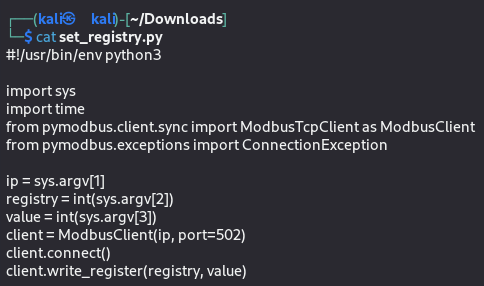


Utilizando o comando “cat”para visualizar o conteúdo do script “discovery.py”, há a função “read\_holding\_register”.



## Which is the function used to write holding registers in the pymodbus library?

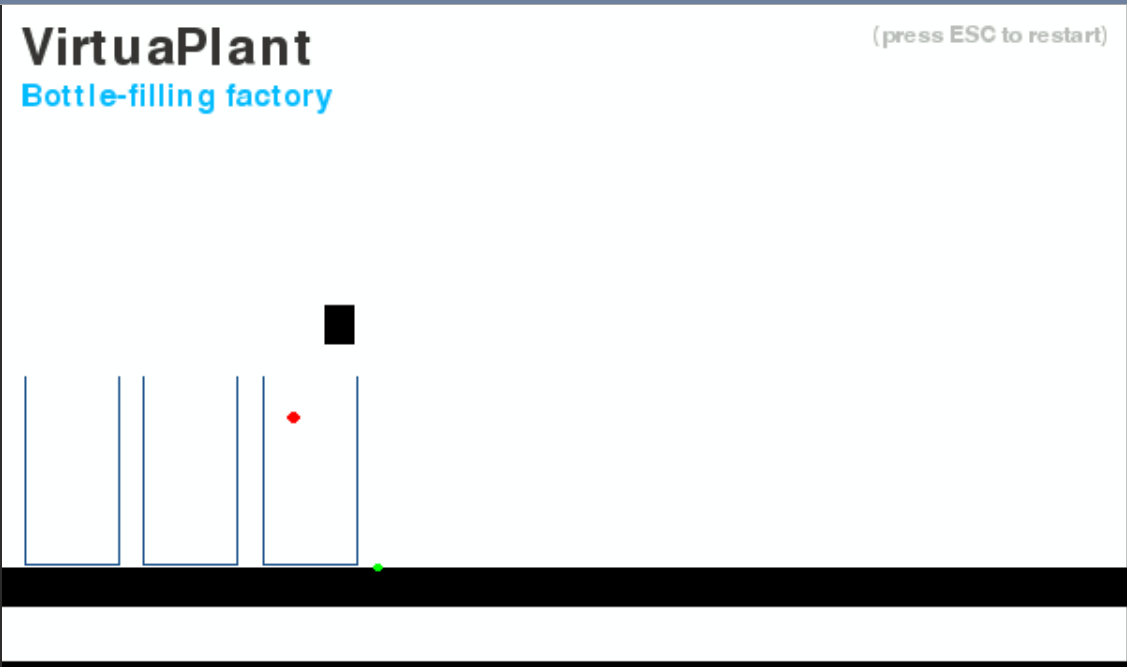
Realizando o mesmo processo da pergunta anterior, mas com script “set\_registry.py”, há a função “write\_register”.



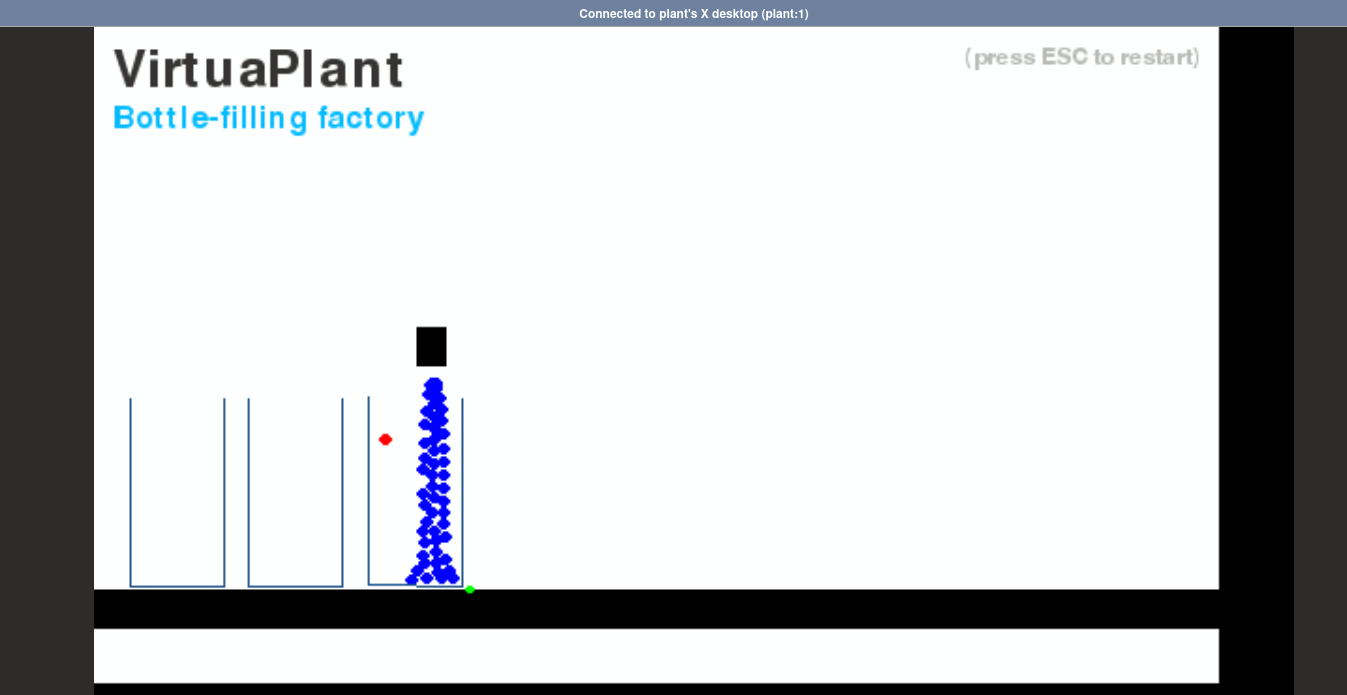
## How many phases can we observe?

É possível observar três fases:

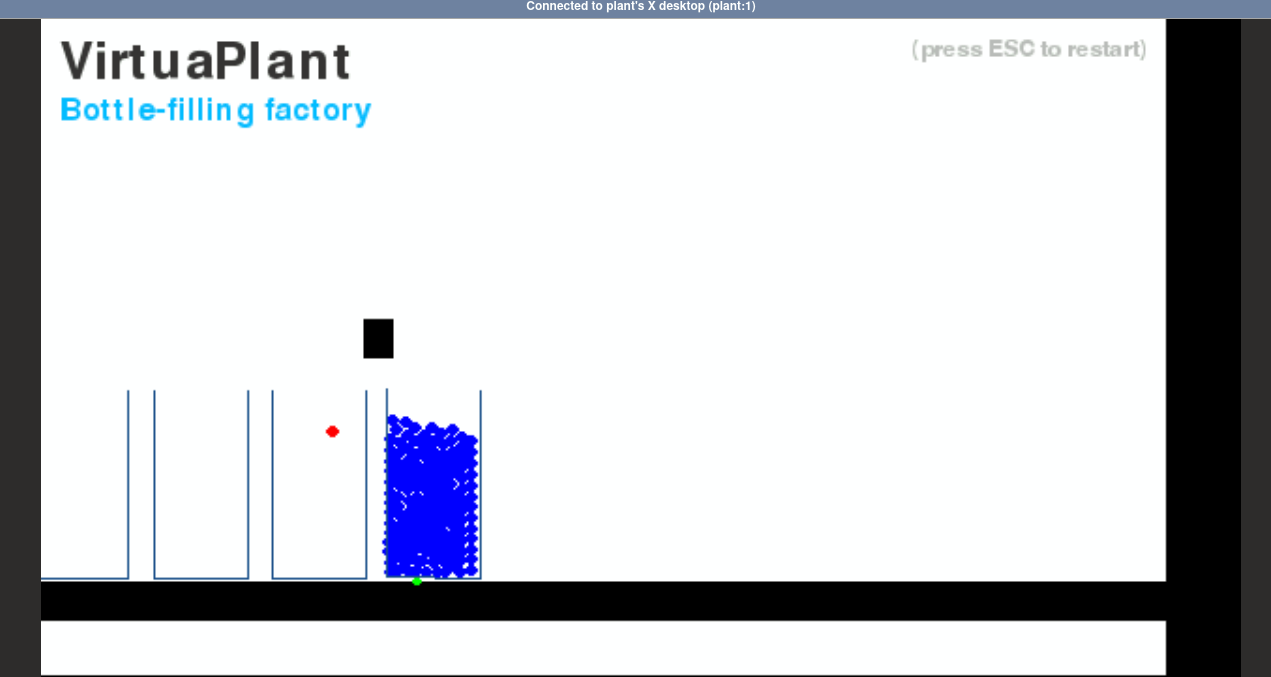
A inicialização, em que a primeira garrafa é levada até o bocal:



O enchimento da garrafa:



Movimento após o enchimento da garrafa até a próxima garrafa vazia:



## How many sensors can we observe?

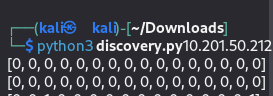
Sensores são usados para ler o estado atual de uma planta. Logo, são observados dois sensores: o responsável por detectar se a garrafa vazia está abaixo do bocal e o responsável por detectar o nível da água.

## How many actuators can we observe?

Atuadores são usados para alterar o estado atual da planta. Logo, são observados três atuadores: o botão de ligar/desligar a planta, o responsável por abrir ou fechar o bocal e o responsável por parar ou continuar o movimento da esteira.

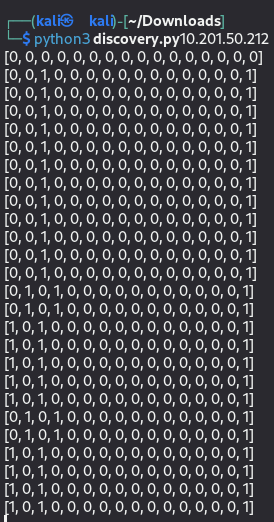
## Using the script discovery.py, how many registers can we count?

No total são 16 registros.



## After the plant is started and a bottle is loaded, how many registers are continuously changing their values?

Após a planta ser iniciada e a primeira garrafa ser enchida, os quatro primeiros registros mudam constantemente os seus valores.



## Which is the minimum observed value?

O valor mínimo observado é zero.

## Which is the maximum observed value?

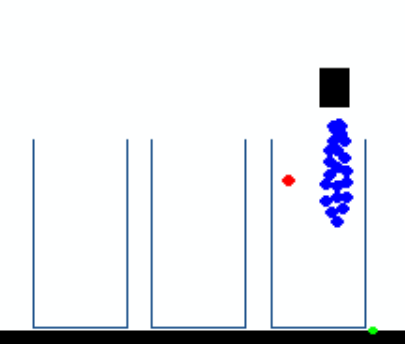
O valor máximo observado é o um.

## Which registry is holding its value?

O décimo sexto registro não altera o seu valor após a inicialização.

## Which registries are set to 1 while the nozzle is filling a bottle?

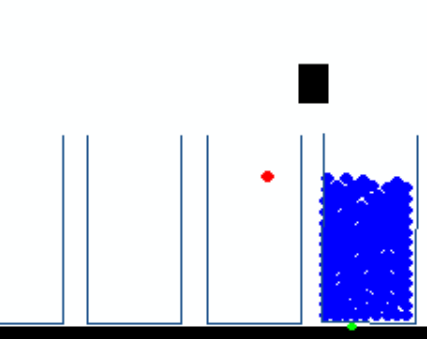
Enquanto a garrafa está sendo enchida, os registros 2 e 4 são alterados para 1.





## Which registries are set to 1 while the roller is moving the bottles?

Enquanto a esteira está movimentando as garrafas, os registros 1 e 3 são alterados para 1.





## Which is the color of the water level sensor?

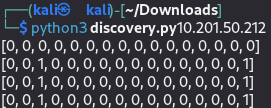
A cor do sensor do nível de água é vermelha.

## Which is the color of the bottle sensor?

A cor do sensor do da garrafa é verde.

## If you observe the plant at the very beginning, which is the registry associated with the roller?

O registro associado com a esteira é o terceiro.



## Based on the previous answer, which is the registry associated with the water level sensor?

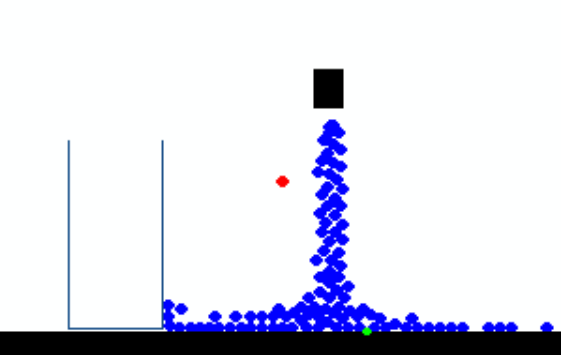
O registro associado com o sensor do nível de água é o primeiro.



## Which is the registry associated with the nozzle?

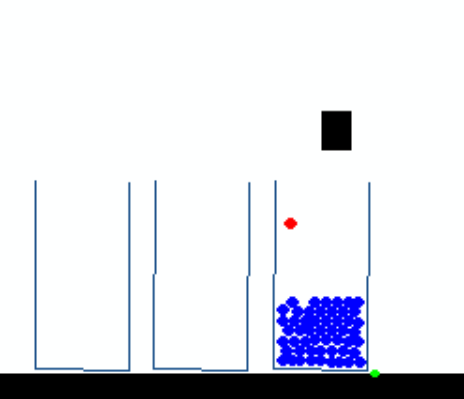
Após realizar os testes alterando os registros com o script “set\_registry.py”, descobre-se que o registro associado com o bocal é o quarto





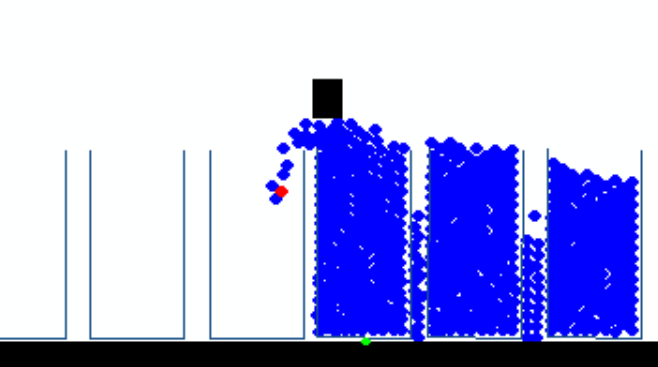
## Shutdown the plant and avoid the plant manager starts it again.





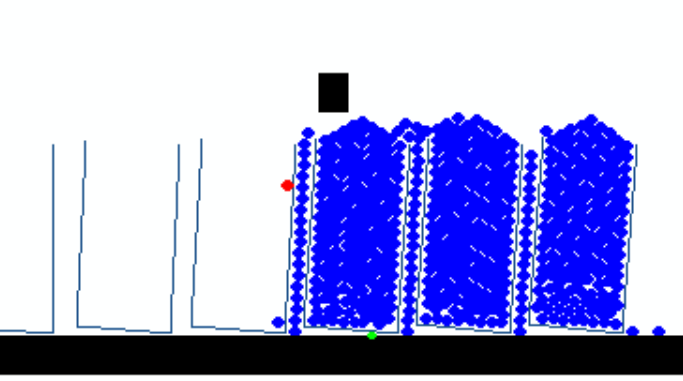
## Start the plant, open the nozzle while bottles are moving.



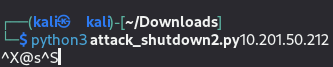


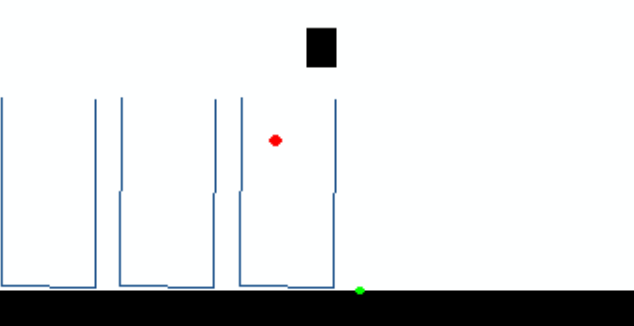
## Start the plant, open the nozzle and stop the roller.





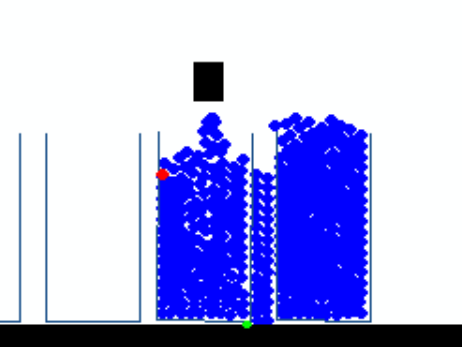
## Repeat attack in question 1 abusing sensor registries.





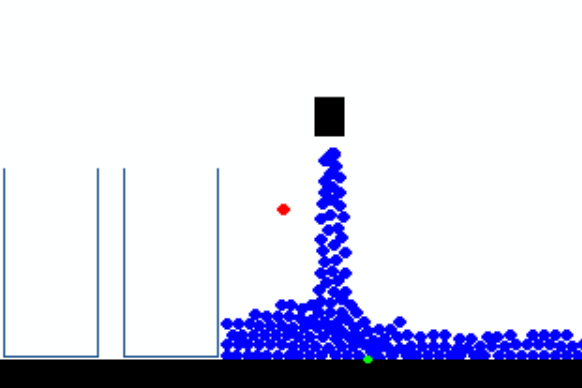
## Repeat attack in question 2 abusing sensor registries.





## Repeat attack in question 3 abusing sensor registries.





# Conclusão

O CTF oferece ao estudante uma base introdutória sólida, sobre OT/ICS, SCADA e protocolo Modbus. Além disso, por meio de uma simulação prática, visual, é possível compreender, ainda que de maneira simplificada, como um ataque a um Sistema de Controle Industrial corre e quais são suas possíveis consequências para o ambiente industrial.

# Referências

Todas as informações utilizadas estavam disponíveis no próprio CTF: https://tryhackme.com/room/attackingics1