Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Attacking ICS Plant #1 - TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Attacking ICS Plant #1 – Larissa Gomes |
| **N° Revisão** | 1 |
| **Data de publicação** | 30/10/2025 |
| **Link** | <https://tryhackme.com/room/attackingics1> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Larissa Gomes | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 06/10/2025 | Produção |
| **1** | 30/10/2025 | Coordenador |
| **2** | 30/10/2025 | Coordenador |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Sistemas de controle industrial (ICS), Tecnologia operacional (OT), Sistemas SCADA, Protocolo modbus (Modicon / Schneider Electric). |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 4](#_Toc210642716)

[Desenvolvimento 4](#_Toc210642717)

[Which is the function used to read holding registers in pymodbus library? 4](#_Toc210642718)

[Which is the function used to write holding registers in pymodbus library? 4](#_Toc210642719)

[How many phases can we observe? 5](#_Toc210642720)

[How many sensors can we observe? 5](#_Toc210642721)

[How many actuators can we observe? 6](#_Toc210642722)

[Using the script discovery.py, how many registers can we count? 6](#_Toc210642723)

[After the plant is started and a bottle is loaded, how many registers are continuously changing their values? 7](#_Toc210642724)

[Which is the minimum observed value? 7](#_Toc210642725)

[Which is the maximum observed value? 8](#_Toc210642726)

[Which registry is holding its value? 8](#_Toc210642727)

[Which registries are set to 1 while the nozzle is filling a bottle? 9](#_Toc210642728)

[Which registries are set to 1 while the roller is moving the bottles? 9](#_Toc210642729)

[Which is the color of the water level sensor? 9](#_Toc210642730)

[Which is the color of the bottle sensor? 10](#_Toc210642731)

[If you observe the plant at the very beginning, which is the registry associated with the roller? 10](#_Toc210642732)

[Based on the previous answer, which is the registry associated with the water level sensor? 10](#_Toc210642733)

[Which is the registry associated with the nozzle? 11](#_Toc210642734)

[Conclusão 11](#_Toc210642735)

[Referências 11](#_Toc210642736)

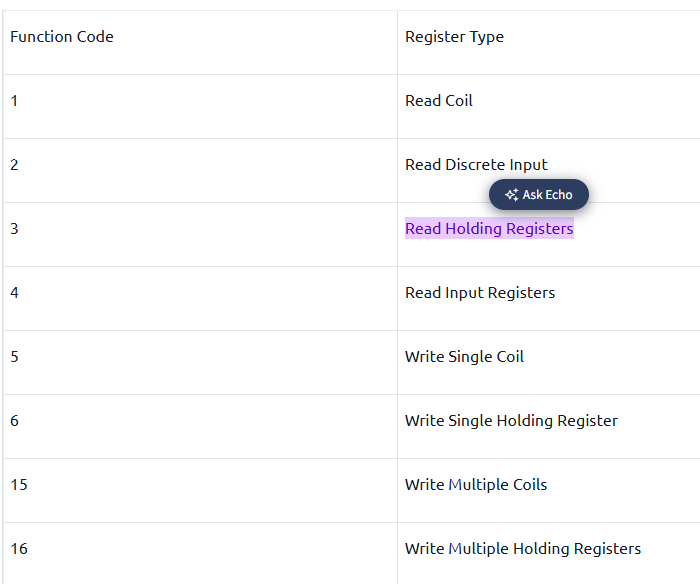
Contextualização

AttackingICS#1 é um CTF da plataforma TryHackMe que tem o intuito de ensinar como descobrir e atacar plantas ICS usando o protocolo *modbus* (Modicon / Schneider Electric).

Desenvolvimento

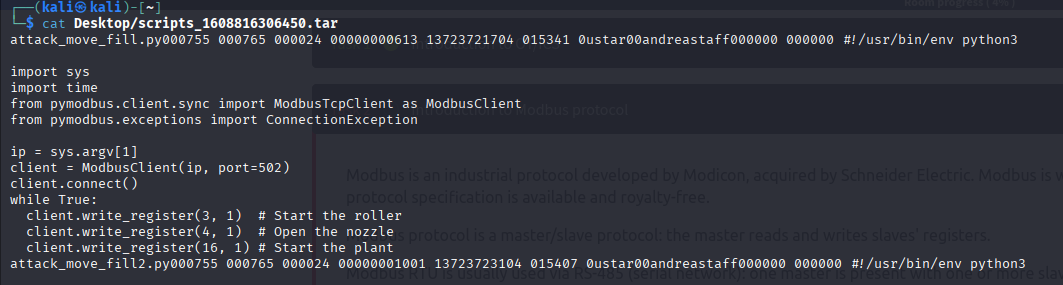
Which is the function used to read holding registers in pymodbus library?

Leia o texto de apoio, assim será possível descobrir qual é a função utilizada para ler registradores na biblioteca *pymodbus*.



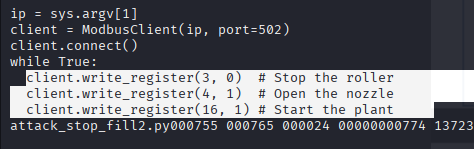
Which is the function used to write holding registers in pymodbus library?

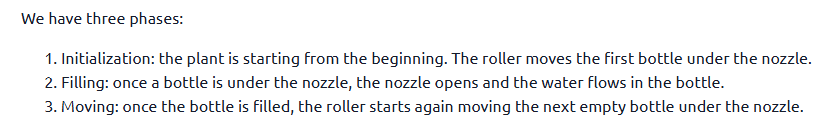
Baixe o arquivo dado no CTF, abra ele e procure onde no script Python dado foi utilizada a função para escrever registradores de retenção.

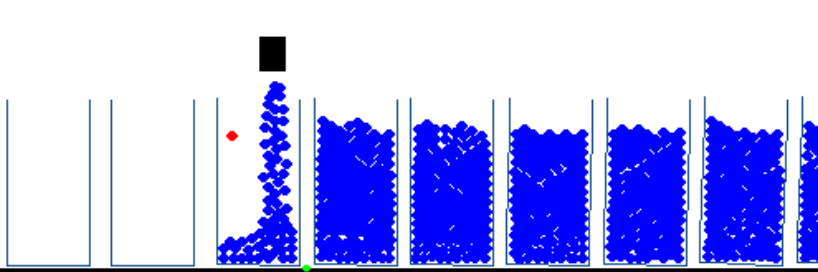


How many phases can we observe?

Procure no script dado pelo CTF e nas informações dadas, com isso é possível encontrar quantas fases são escritas/registradas.

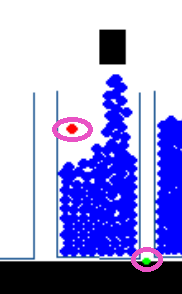






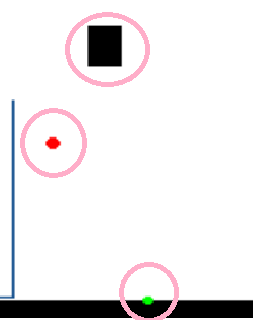
How many sensors can we observe?

Observe o desenvolvimento da planta e com base na definição de sensores dado pelo CTF é possível descobrir dois sensores.



How many actuators can we observe?

Observe o desenvolvimento da planta e com base na definição de atuadores dado pelo CTF é possível descobrir três atuadores



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

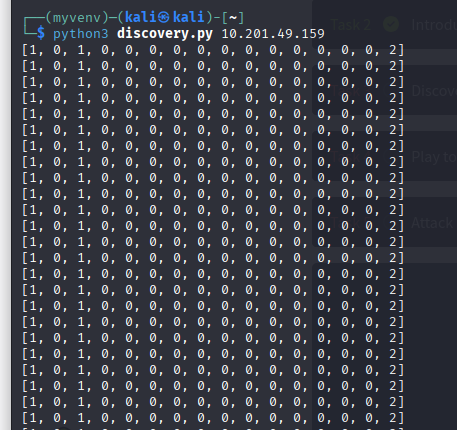
Com o script baixado, separe-o utilizando o seguinte comando:

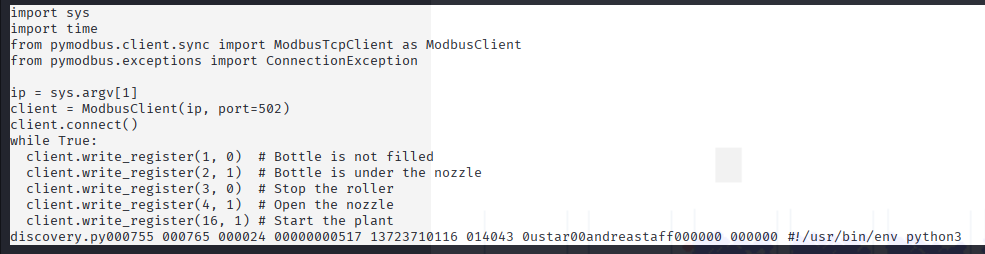
**tar -xvf <nome do arquivo>**

Agora com os arquivos python separados, rode o script discover.py utilizando o comando;

**Python3 discover.py <IP>**

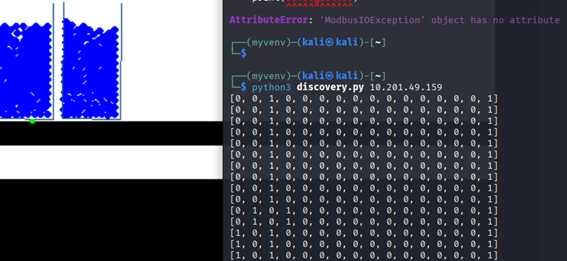
Observe o código e o script que está rodando e assim descubra que da para se contar 16 registradores.

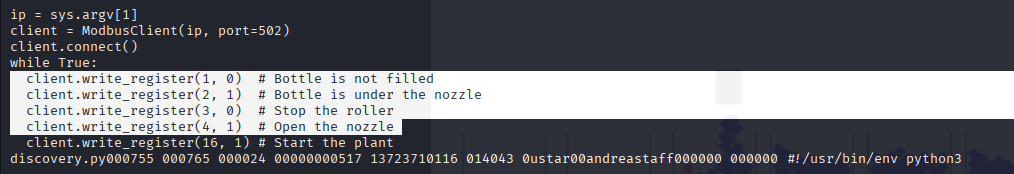




After the plant is started and a bottle is loaded, how many registers are continuously changing their values?

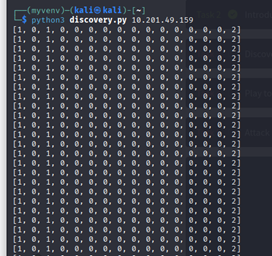
Observe o código e o script que está rodando, assim é possível descobrir que quatro registros estão continuamente alterando seus valores.





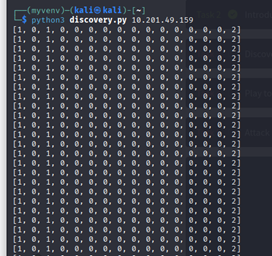
Which is the minimum observed value?

Observe o script que está rodando assim é possível descobrir o valor mínimo observado, sendo ele “0”.



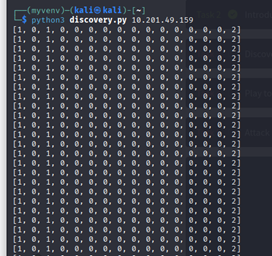
Which is the maximum observed value?

Observe o script que está rodando assim é possível descobrir o valor mínimo observado, sendo ele “1”.



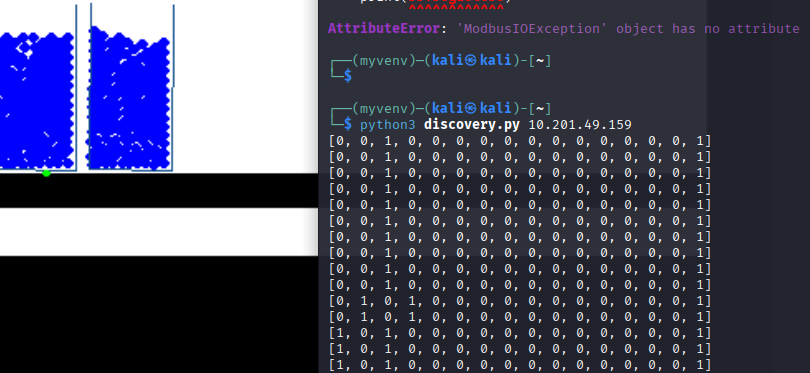
Which registry is holding its value?

Observe o script que está rodando assim é possível descobrir qual é o registro que está mantendo o seu valor inicial.



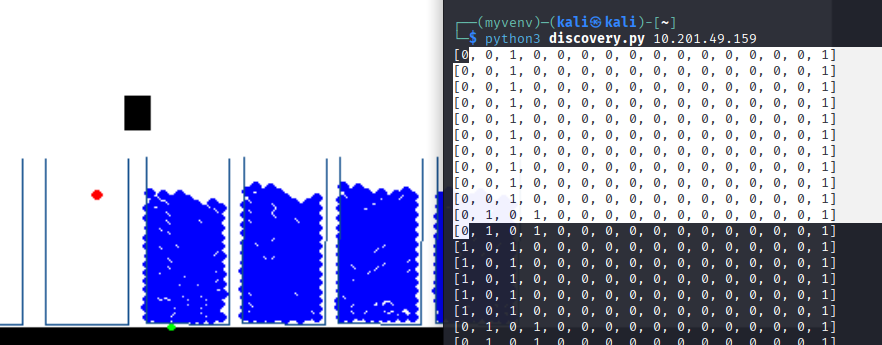
Which registries are set to 1 while the nozzle is filling a bottle?

Observe a planta e o script simultaneamente, assim será possível identificar quais registros são definidos como 1 quando o bico está enchendo a garrafa.



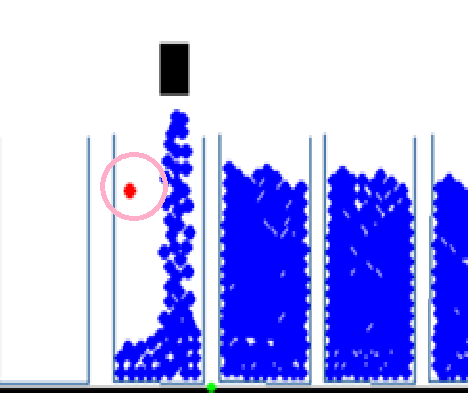
Which registries are set to 1 while the roller is moving the bottles?

Observe a planta e o script simultaneamente, assim será possível identificar quais registros são definidos como 1 quando o rolo está movendo as garrafas.



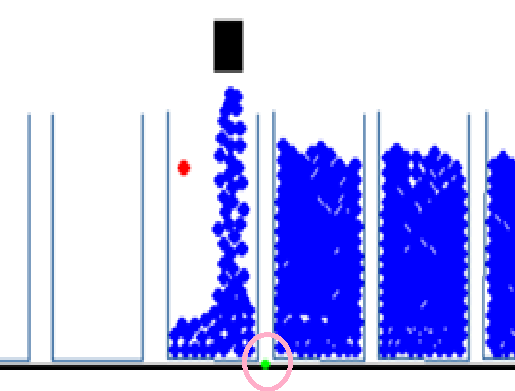
Which is the color of the water level sensor?

Observe a planta e veja qual é a cor do sensor de nível de água.



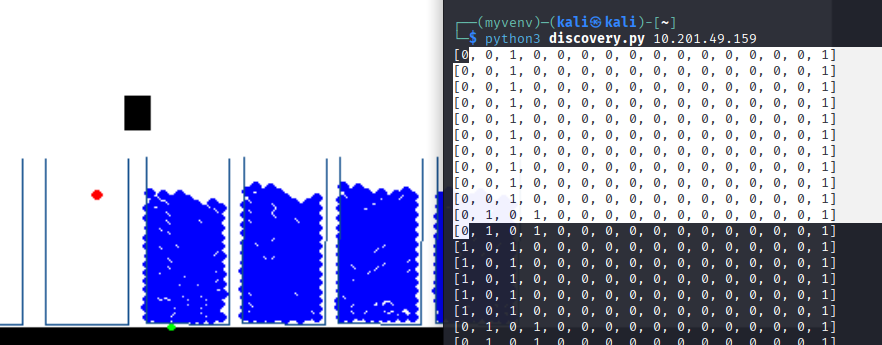
Which is the color of the bottle sensor?

Observe a planta e veja qual é a cor do sensor da garrafa.



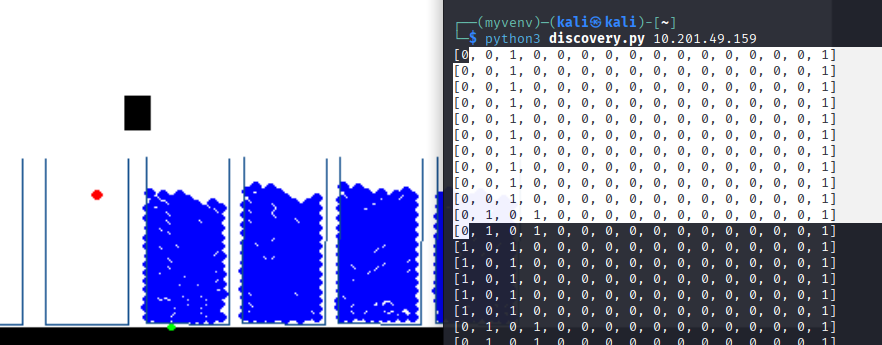
If you observe the plant at the very beginning, which is the registry associated with the roller?

Observe a planta e o script simultaneamente, assim será possível identificar qual registro é associado ao rolo.



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

Observe a planta e o script simultaneamente, assim será possível identificar qual registro é associado ao nível de água.

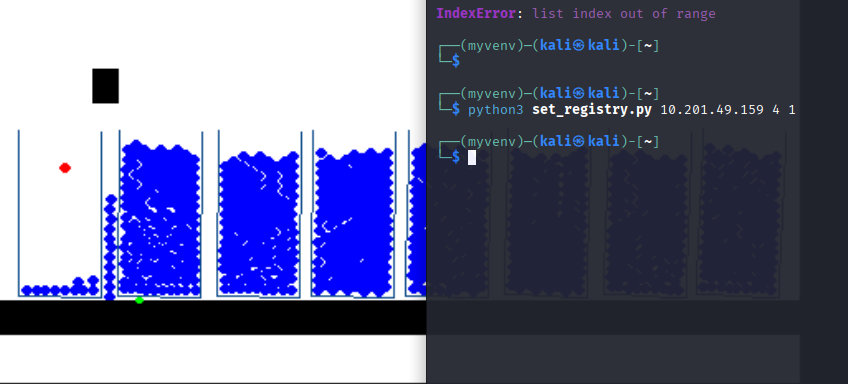


Which is the registry associated with the nozzle?

Usando o comando:

**Python3 set\_registery.py <IP> <registro> <0/1(1 = ligado, 0 = desligado)>**

É possível ir alterando os valores dos registros, assim é possível descobrir qual registro é associado ao bico.



Conclusão

O desafio de " Attacking ICS Plant #1 “da plataforma TryHackMe foi uma excelente oportunidade para praticar e aprender sobre OT/ICS. O documento detalha as etapas seguidas para a resolução do CTF, que abordou conceitos como sistemas de controle industrial (ICS), tecnologia operacional (OT), sistemas SCADA e protocolo modbus (Modicon / Schneider Electric).

Referências

<https://www.csimn.com/CSI_pages/Modbus101.html>

<https://chatgpt.com/> - Utilizado para dúvidas e estudo.