Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Attacking ICS Plant #1 – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Attacking ICS Plant #1 – Pedro Leal Ariosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 03/09/2025 |
| **Link** | https://tryhackme.com/room/attackingics1 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Pedro Leal Ariosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 03/09/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | OT |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Which is the function used to read holding registers in pymodbus library? 3](#_heading=h.3znysh7)

[Which is the function used to write holding registers in pymodbus library? 3](#_heading=h.2et92p0)

How many phases can we observe? 3

How many sensors can we observe? 3

How many actuators can we observe? 3

Using the script discovery.py, how many registers can we count? 4

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

Which is the minimum observed value? 4

Which is the maximum observed value? 4

Which registries are set to 1 while the nozzle is filling a bottle? 4

Which registries are set to 1 while the roller is moving the bottles? 5

Which is the color of the bottle sensor? 5

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

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

Which is the registry associated with the nozzle? 6

Shutdown the plant and avoid the plant manager starts it again 7

Start the plant, open the nozzle while bottles are moving 7

Start the plant, open the nozzle and stop the roller 8

[Conclusão 9](#_heading=h.1t3h5sf)

[Referências 9](#_heading=h.4d34og8)

**Contextualização**

O CTF Attacking ICS Plant busca desenvolver as habilidades e conhecimentos sobre a área de Operational Technology através de uma simulação do funcionamento de uma indústria produtora de garrafas de água. O objetivo do CTF é demonstrar quão vulneráveis as máquinas e dispositivos essenciais da indústria estão e quão impactante pode ser caso um atacante conseguisse acesso a esses dispositivos.

**Desenvolvimento**

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

De acordo com a tabela fornecida pelo CTF, a função necessária é read holding registers.

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

De acordo com a tabela fornecida pelo CTF, a função necessária é write register.

**How many phases can we observe?**

É possível observar 3 fases no comportamento do circuito: Esteira se movendo, esteira parada com enchimento do recipiente, nível do fluído atinge o sensor para a esteira voltar a andar e repetir o ciclo.

Texto

O conteúdo gerado por IA pode estar incorreto.

Padrão do plano de fundo

O conteúdo gerado por IA pode estar incorreto.

**How many sensors can we observe?**

São 2 sensores existentes para o funcionamento do circuito: sensor de posicionamento do recipiente na esteira e sensor de nível do fluído.

**How many actuators can we observe?**

São 3 atuadores necessários para o funcionamento do sistema: esteira, bocal de saída do fluido e a bomba de água.

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

São 16 registradores de informações, nesse CTF identificados por colunas.

Texto

O conteúdo gerado por IA pode estar incorreto.

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

São 4 registradores que alteram o valor: esteira, sensor de água, sensor de posicionamento e bocal de saída do fluido.

Padrão do plano de fundo

O conteúdo gerado por IA pode estar incorreto.

**Which is the minimum observed value?**

O sistema simulado no CTF utiliza de um sistema binário para interpretar e armazenar as informações. Portanto, 0 é o menor valor observado.

**Which is the maximum observed value?**

O sistema simulado no CTF utiliza de um sistema binário para interpretar e armazenar as informações. Portanto, 1 é o maior valor observado.

**Which registry is holding its value?**

O registrador de número 16 sempre armazena o valor 1.

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

Os registradores 2 e 4 permanecem em nível alto enquanto os recipientes enchem.

Padrão do plano de fundo

O conteúdo gerado por IA pode estar incorreto.

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

Os registradores 1 e 3 permanecem em nível alto enquanto os recipientes enchem.

Texto

O conteúdo gerado por IA pode estar incorreto.

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

A cor do sensor do nível de fluido é vermelho.

Uma imagem contendo Gráfico

O conteúdo gerado por IA pode estar incorreto.

**Which is the color of the bottle sensor?**

A cor do sensor do posicionamento do recipiente na esteira é verde.

Uma imagem contendo Gráfico

O conteúdo gerado por IA pode estar incorreto.

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

O registrador é o 3.

Texto

O conteúdo gerado por IA pode estar incorreto.

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

O registrador do nível de fluido é o 1, uma vez que apresenta nível baixo quando identifica passagem do fluido.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Which is the registry associated with the nozzle?**

É o registrador 4.

Padrão do plano de fundo

O conteúdo gerado por IA pode estar incorreto.

**Shutdown the plant and avoid the plant manager starts it again**

Com o comando “python3 attack\_shutdown.py ip” foi possível desativar a planta.



Uma imagem contendo Gráfico

O conteúdo gerado por IA pode estar incorreto.

**Start the plant, open the nozzle while bottles are moving**

Com o comando “python3 attack\_move\_fill2.py ip” foi possível manter a esteira em movimento e desativar o sensor de posicionamento da esteira. Assim, o sistema começou a inundar.

Texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

**Start the plant, open the nozzle and stop the roller**

Com o comando “python3 attack\_move\_fill2.py ip” e “python3 attack\_stop\_fill.py ip” foi possível abrir o bocal e parar a esteira.

Texto

O conteúdo gerado por IA pode estar incorreto.



Gráfico, Gráfico de dispersão

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

De maneira completa e extremamente didática, o CTF conseguiu abordar todos os tópicos da área de OT de maneira detalhada e precisa, abordando tópicos como atuadores, registradores, sensores e os possíveis impactos ocasionados por uma invasão.

**Referências**

https://edgeglobal.com.br/blog/sensores-e-atuadores/

https://upkeep.com/learning/whats-the-difference-between-sensors-and-actuators/