Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Attacking ICS Plant #1 – TryHackMe

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

|  |  |  |
| --- | --- | --- |
| **Redação** | Nicolas Mota Engles | 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, Modbus |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_Toc208172517)

[Desenvolvimento 3](#_Toc208172518)

[“Which is the function used to read holding registers in pymodbus library?” (Qual é a função utilizada para ler registradores de holding no pymodbus?) 3](#_Toc208172519)

[“Which is the function used to write holding registers in pymodbus library?” (Qual é a função utilizada para escrever registradores de holding no pymodbus?) 4](#_Toc208172520)

[How many phases can we observe? (Quantas fases podemos observar?) 4](#_Toc208172521)

[How many sensors can we observe? (Quantos sensores podemos observar?) 5](#_Toc208172522)

[How many actuators can we observe? (Quantos atuadores podemos observar?) 5](#_Toc208172523)

[Using the script discovery.py, how many registers can we count? (Utilizando o script discovery.py, quantos registros podemos contar?) 5](#_Toc208172524)

[After the plant is started and a bottle is loaded, how many registers are continuously changing their values? (Após o início da linha de produção e o enchimento de uma garrafa, quantos registros têm seus valores constantemente alterados?) 6](#_Toc208172525)

[Which is the minimum observed value? (Qual é o valor mínimo observado?) 6](#_Toc208172526)

[Which is the maximum observed value? (Qual é o valor máximo observado?) 6](#_Toc208172527)

[Which registry is holding its value? (Qual registro contém esse valor?) 6](#_Toc208172528)

[Which registries are set to 1 while the nozzle is filling a bottle? (Quais registros possuem valor 1 enquanto a garrafa está sendo enchida?) 6](#_Toc208172529)

[Which registries are set to 1 while the roller is moving the bottles? (Quais registros possuem o valor 1 enquanto a esteira move as garrafas?) 7](#_Toc208172530)

[Which is the color of the water level sensor? (Qual é a cor do sensor de nível da água?) 7](#_Toc208172531)

[Which is the color of the bottle sensor? (Qual é a cor do sensor de posição da garrafa?) 7](#_Toc208172532)

[If you observe the plant at the very beginning, which is the registry associated with the roller? (Observando a linha de produção desde o ínicio, qual é o registro associado à esteira?) 7](#_Toc208172533)

[Based on the previous answer, which is the registry associated with the water level sensor? (Baseando-se na resposta à questão anterior, qual registro está associado ao sensor de nível da água?) 7](#_Toc208172534)

[Which is the registry associated with the nozzle? (Qual é o registro associado ao dispensador de água?) 7](#_Toc208172535)

[Conclusão 8](#_Toc208172536)

[Referências 10](#_Toc208172537)

Contextualização

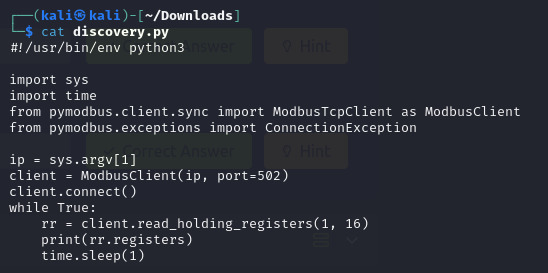
“Attacking ICS Plant #1” é um desafio de OT/ICS que consiste em explorar vulnerabilidades do protocolo *Modbus* afim de interromper o funcionamento de uma linha de produção de garrafas de água.

Desenvolvimento

“Which is the function used to read holding registers in pymodbus library?” (Qual é a função utilizada para ler registradores de holding no pymodbus?)

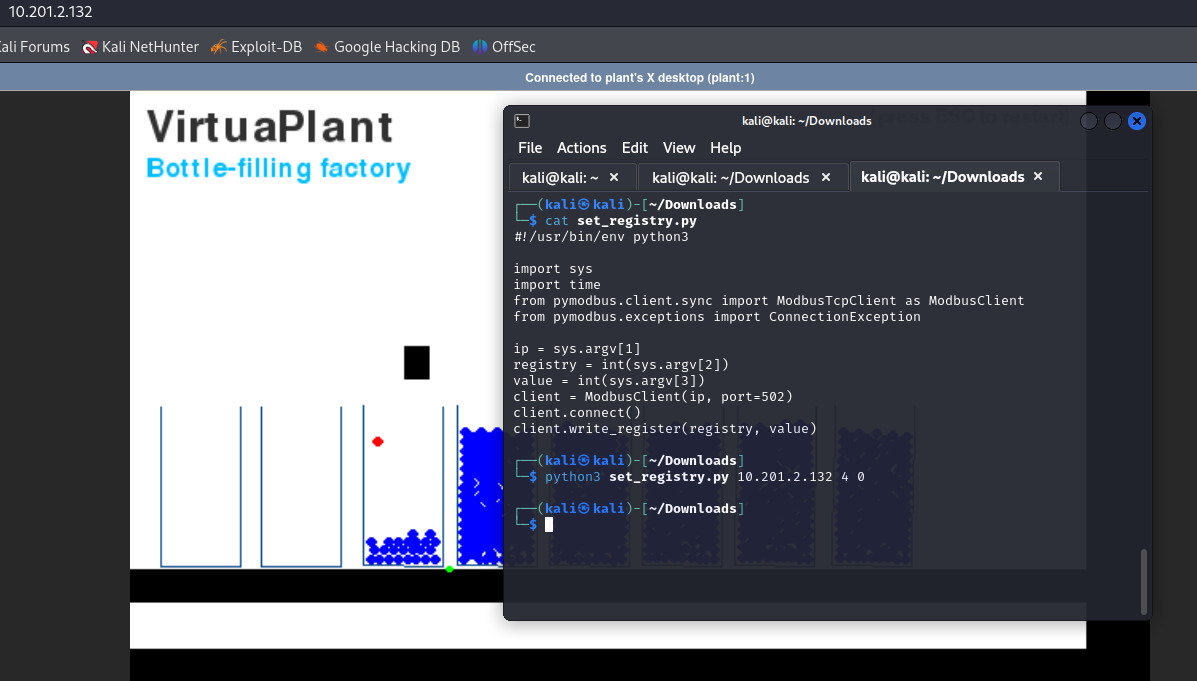
Dentro da biblioteca pymodbus, o arquivo discovery.py é o que contêm essa função.

Resposta: “read\_holding\_registers”



“Which is the function used to write holding registers in pymodbus library?” (Qual é a função utilizada para escrever registradores de holding no pymodbus?)

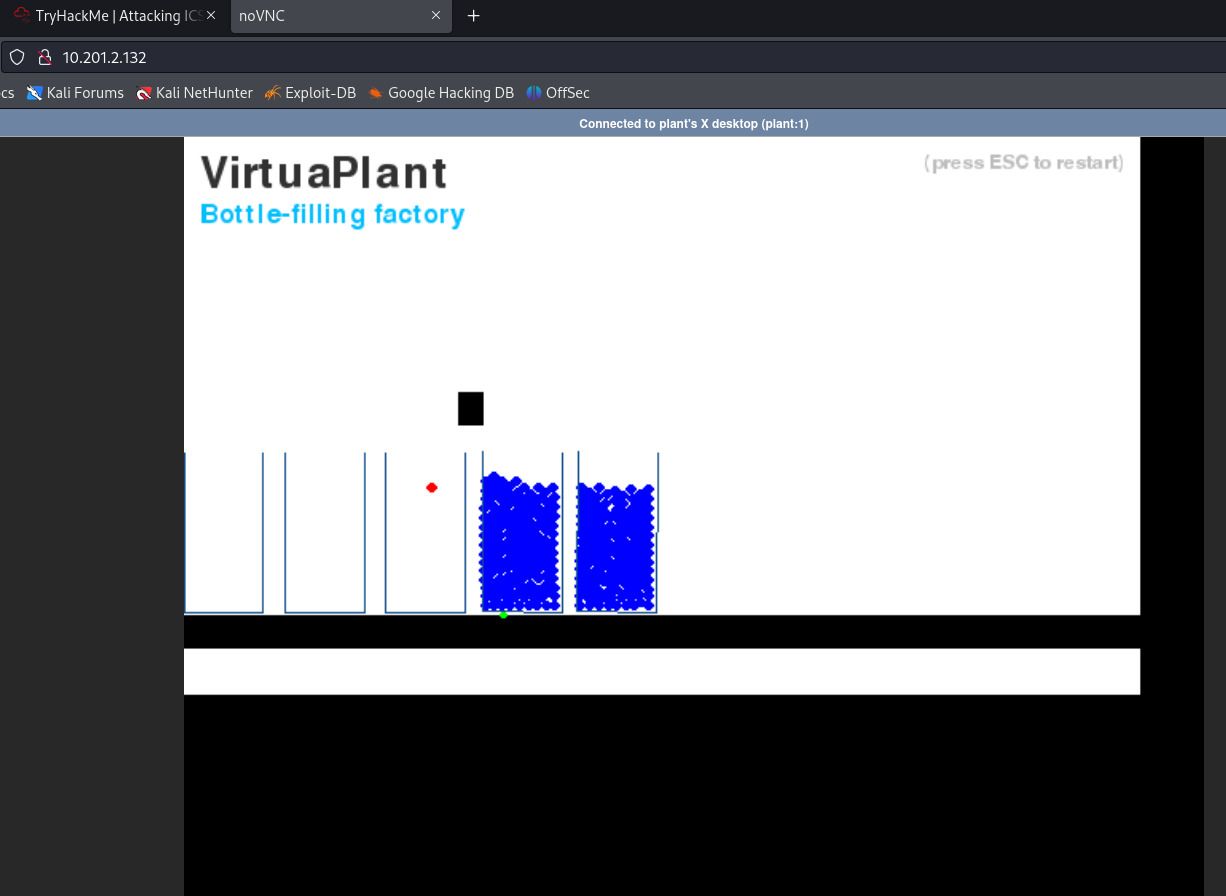
Diferente da função anterior, essa tem um formato diferente, não especificando o tipo de registro que é escrito por ela. Pode ser encontrada no arquivo set\_registry.py



How many phases can we observe? (Quantas fases podemos observar?)

Podemos responder essa pergunta abrindo o visualizador da linha de produção somente observando como ela funciona.

Resposta: 3



How many sensors can we observe? (Quantos sensores podemos observar?)

Da mesma maneira, observando a linha de produção (vide imagem da pergunta anterior), é possível observar uma bolinha vermelha (sensor de nível da água) e outra verde (sensor de posição da garrafa).

Resposta: 2

How many actuators can we observe? (Quantos atuadores podemos observar?)

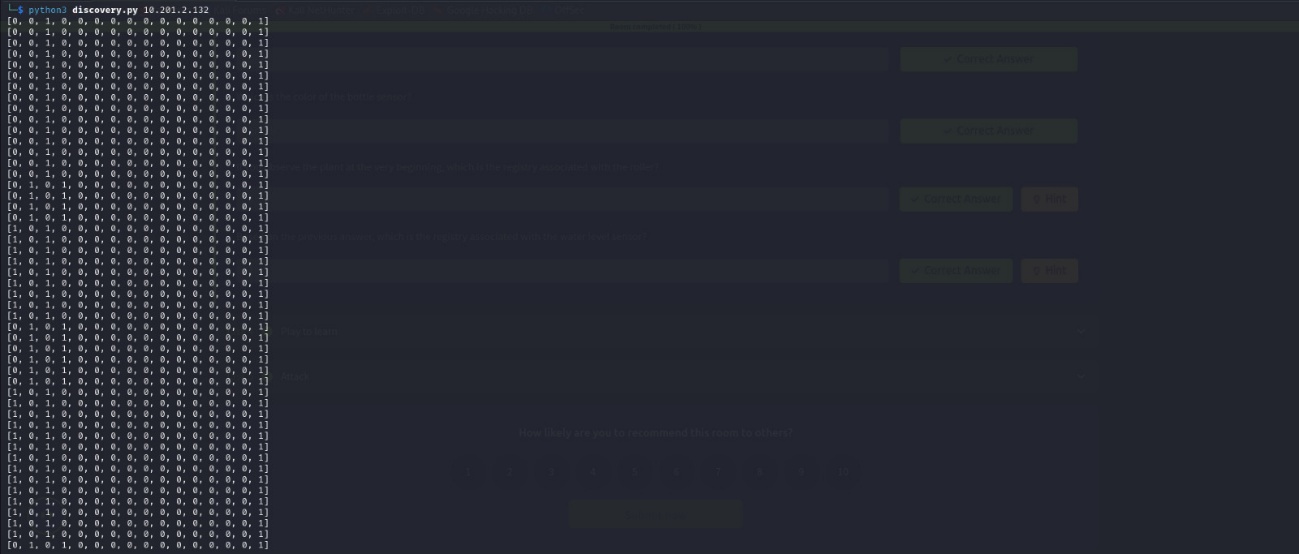
Um atuador é um dispositivo que recebe um sinal de controle e, em resposta, realiza alguma ação sobre o processo da linha de produção. Além dos dois sensores, há também o botão de iniciar/encerrar a linha de produção.

Resposta: 3

Using the script discovery.py, how many registers can we count? (Utilizando o script discovery.py, quantos registros podemos contar?)

Executando o script discovery.py com o enderço IP da linha de produção, recebemos uma matriz 1x16, onde cada elemento representa o valor de um registro.

Resposta: 16



After the plant is started and a bottle is loaded, how many registers are continuously changing their values? (Após o início da linha de produção e o enchimento de uma garrafa, quantos registros têm seus valores constantemente alterados?)

Observa-se na matriz de registros (vide imagem da questão anterior) que os registros 1, 2, 3 e 4 contantemente mudam seus valores, com todos os outros registros permanecendo inalterados.

Resposta: 4

Which is the minimum observed value? (Qual é o valor mínimo observado?)

Observando novamente a matriz (vide imagem da questão anteanterior), percebe-se que todos os registros são binários, ou seja, possuem valor 0 ou 1.

Resposta: 0

Which is the maximum observed value? (Qual é o valor máximo observado?)

Vide desenvolvimento da resposta à questão anterior.

Resposta: 1

Which registry is holding its value? (Qual registro contém esse valor?)

Os registros 1, 2, 3 e 4 todos contém o valor 1 em algum momento durante o funcionamento da linha de produção. Porém apenas o registro de número 16 contém esse intermitentemente.

Resposta: 16

Which registries are set to 1 while the nozzle is filling a bottle? (Quais registros possuem valor 1 enquanto a garrafa está sendo enchida?)

Analizando a matriz de registros e o visualizador da linha de produção simultaneamente, é possível observar que os registros 2 e 4 têm seus valores alterados para 1 enquanto a garrafa está sendo enchida.

Resposta: 2, 4

Which registries are set to 1 while the roller is moving the bottles? (Quais registros possuem o valor 1 enquanto a esteira move as garrafas?)

Analizando a matriz de registros e o visualizador da linha de produção simultaneamente, é possível observar que os registros 1 e 3 têm seus valores alterados para 1 enquanto a esteira se move.

Resposta: 1, 3

Which is the color of the water level sensor? (Qual é a cor do sensor de nível da água?)

Observando o visualizador da linha de produção, percebe-se que o único sensor que poderia possívelmente estar detectando o nível da água é o de cor vermelha.

Resposta: red (vermelho)

Which is the color of the bottle sensor? (Qual é a cor do sensor de posição da garrafa?)

Há dois sensores: se o vermelho é o de nível da água, o outro só pode ser o de posição da garrafa.

Resposta: green (verde)

If you observe the plant at the very beginning, which is the registry associated with the roller? (Observando a linha de produção desde o ínicio, qual é o registro associado à esteira?)

Observa-se, ao iniciar a linha de produção, que a esteira está se movendo e o único registro com valor 1, além do registro de número 16, é o registro de número 3.

Resposta: 3

Based on the previous answer, which is the registry associated with the water level sensor? (Baseando-se na resposta à questão anterior, qual registro está associado ao sensor de nível da água?)

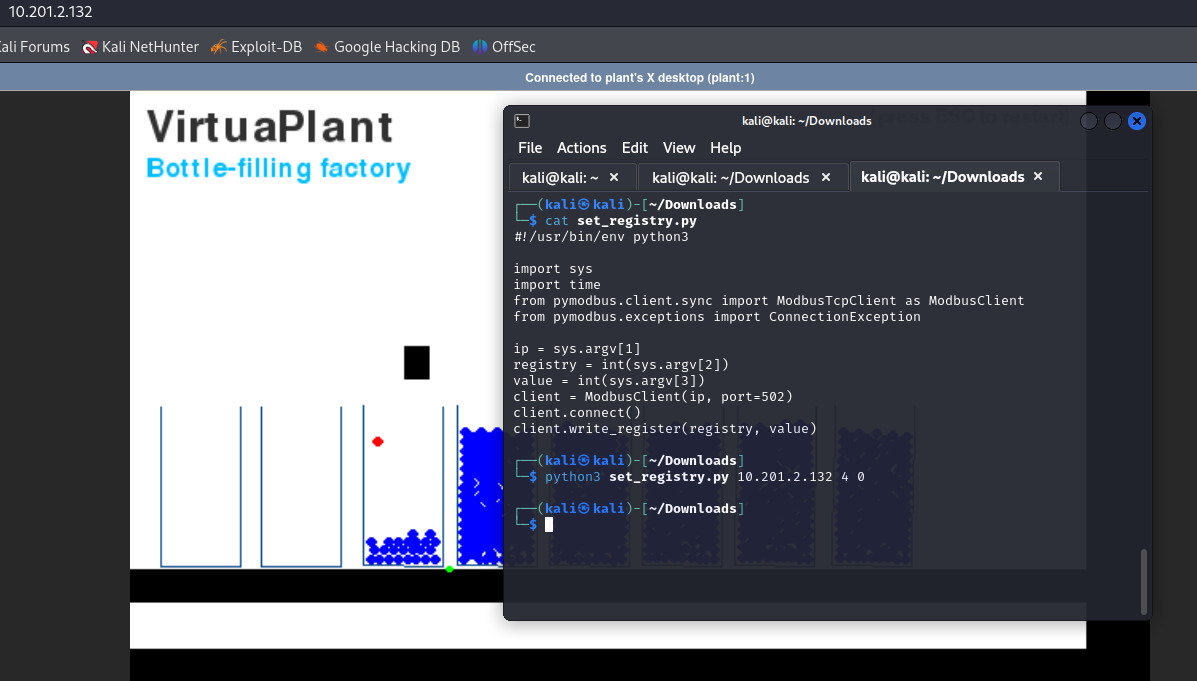
Considerando que a esteira só irá se mover após o enchimento da garrafa, observa-se que, exceto no ínicio do processo, o registro de número 1 possui valor 1 apenas quando o registro da esteira também possui valor 1.

Resposta: 1

Which is the registry associated with the nozzle? (Qual é o registro associado ao dispensador de água?)

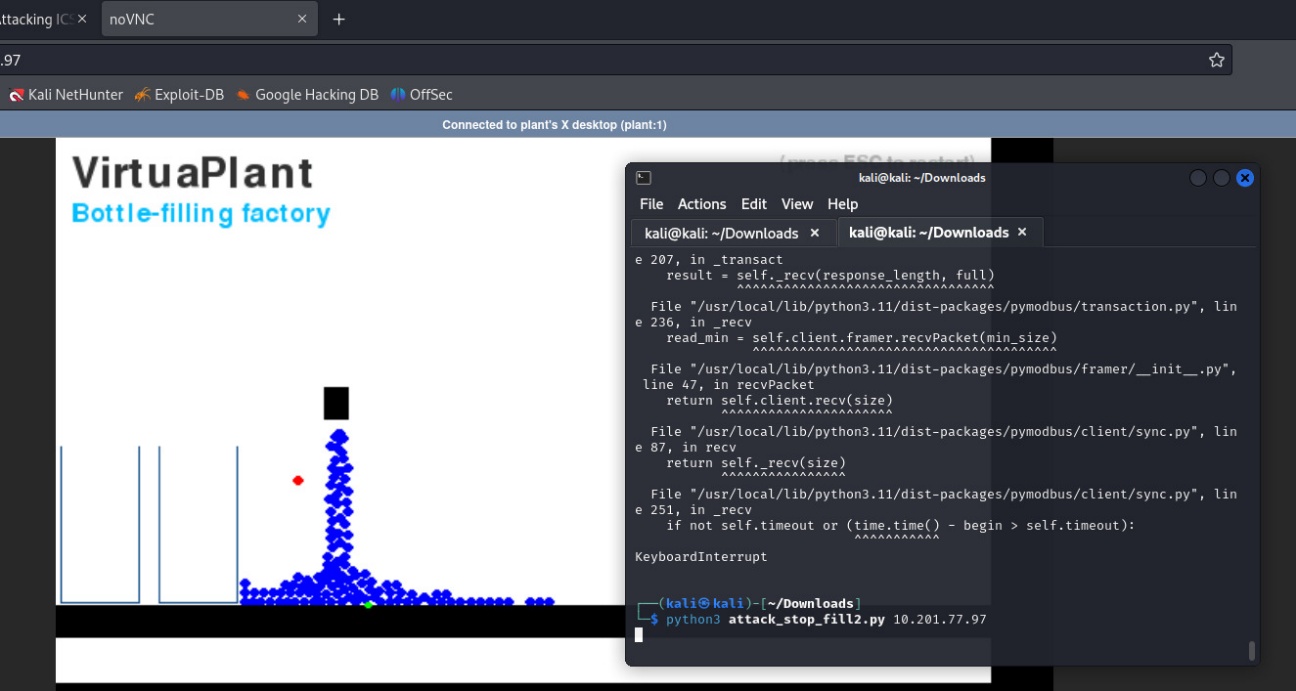
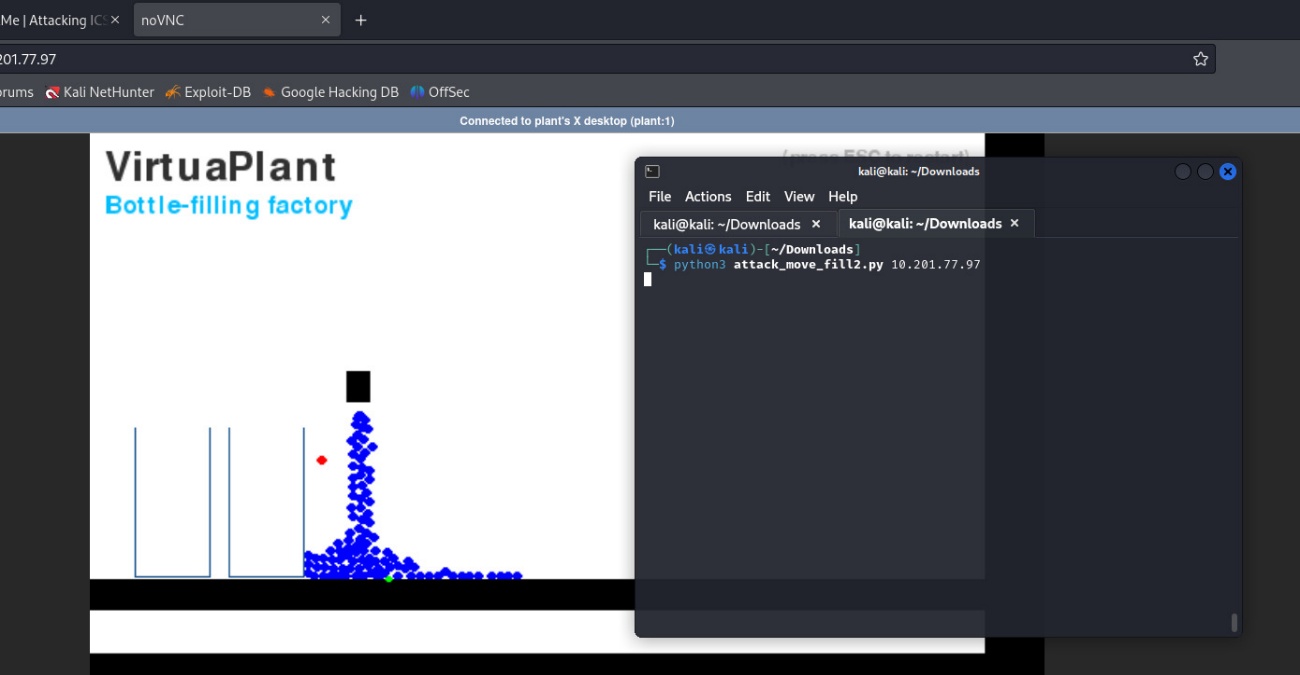
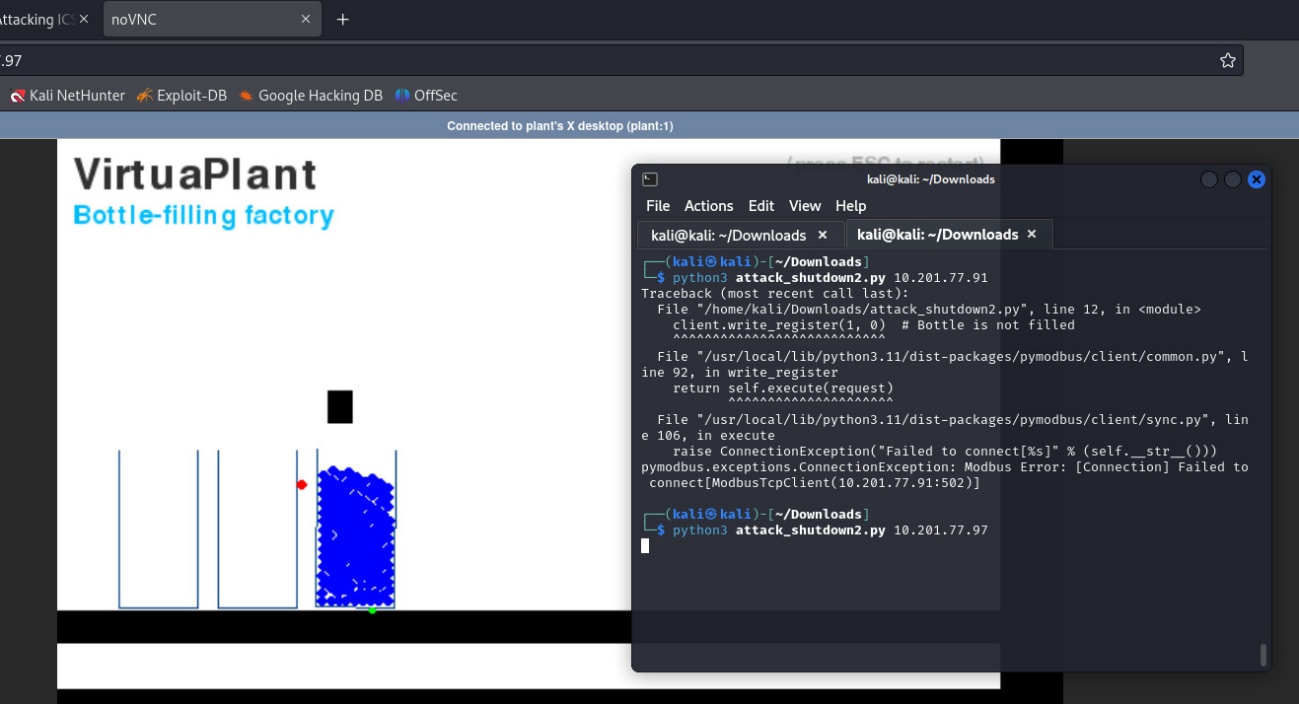
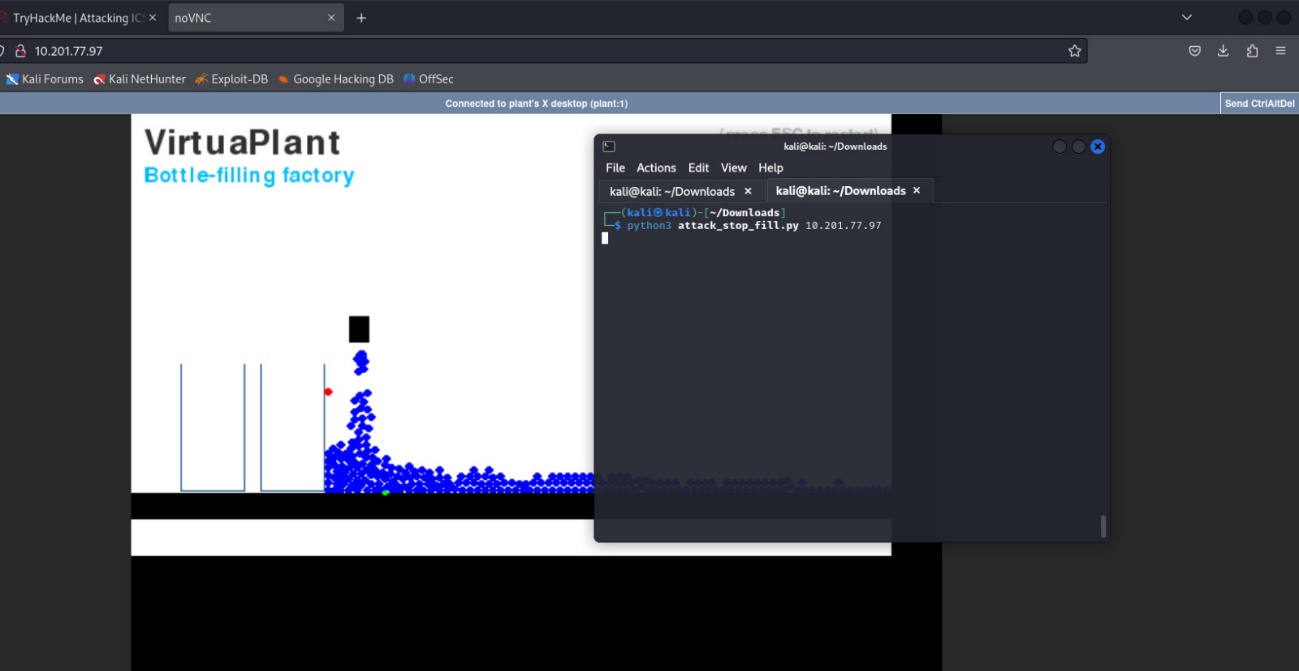
Utilizando o script set\_registry.py, é possível alterar o valor do registro número 4 para 0 enquanto a garrafa está sendo enchida, o que fará com que o dispensador pare de funcionar, interrompendo assim a linha de produção.

Resposta: 4



Conclusão

O materal fornecido para o desafio dispõe de alguns scripts que são utilizados somente para atacar a linha de produção. Esses usufruem das mesmas funções que o script set\_registry.py, porém de maneira pré-definida e com uma finalidade exclusiva.



Esse CTF demonstra de maneira clara e prática como um ataque cibernético relativamente simples pode causar danos enormes à indústria, demonstrando assim a importância da segurança em OT.

Referências

[Google Gemini](https://gemini.google.com/)