Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

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

|  |  |  |
| --- | --- | --- |
| **Redação** | Nome do realizador | Gabriel Lippi da Costa |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | 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)

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

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

[Pergunta 1 3](#_heading=h.3znysh7)

[Pergunta 2 3](#_heading=h.2et92p0)

[Pergunta 3 3](#_heading=h.tyjcwt)

[Pergunta N 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Este relatório detalha as etapas e descobertas do desafio "CTF Attacking ICS Plant #1" no Tryhackme. O desafio é focado em Tecnologia Operacional (OT) e simula uma fábrica de engarrafamento. O objetivo é entender e explorar o sistema usando Python e o protocolo Modbus, que é um protocolo de comunicação comum usado em sistemas de controle industrial.

**Desenvolvimento**

**Tarefa 2: Entendendo o Protocolo Modbus**

Esta tarefa envolve a análise de dois scripts Python para entender como interagir com o sistema de controle industrial simulado.

Lendo os Registros de Retenção (Holding Registers): O script

discovery.py é usado para ler dados do sistema. A função

read\_holding\_registers da biblioteca pymodbus é usada para ler 16 registros a partir do endereço 1. Este é um passo crucial para entender o estado atual dos processos da fábrica.

Escrevendo nos Registros de Retenção (Holding Registers): O script

attack\_move\_fill2.py mostra como escrever dados no sistema para controlar a fábrica. A função

write\_register é utilizada para alterar os valores de registros específicos. O script demonstra como:

* Definir os registros 1 e 2 para

0, indicando que a garrafa não está cheia e não está sob o bico, respectivamente.

* Definir os registros 3 e 4 para

1, o que inicia o rolo e abre o bico.

* Definir o registro 16 para

1, o que inicia toda a planta.

**Tarefa 3: Explorando a Planta de Engarrafamento**

Esta tarefa exige a aplicação do conhecimento adquirido na Tarefa 2 para manipular a operação da fábrica. A imagem fornecida mostra a interface "VirtuaPlant" da fábrica de engarrafamento, destacando componentes-chave como o rolo, a posição da garrafa e o bico. Ao escrever valores específicos nos registros Modbus, como visto no script

attack\_move\_fill2.py, é possível controlar as diferentes etapas do processo de enchimento de garrafas. Isso inclui iniciar e parar o rolo, e abrir e fechar o bico para encher as garrafas.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

O CTF "Attacking ICS Plant #1" oferece uma excelente e acessível introdução à cibersegurança de Tecnologia Operacional. Ele demonstra efetivamente como protocolos comuns como o Modbus podem ser explorados para manipular processos industriais. O uso de scripts Python simples e da biblioteca

pymodbus facilita a compreensão de como os dados são lidos e escritos em um servidor Modbus. Este desafio ressalta a importância de proteger sistemas de controle industrial para evitar acesso não autorizado e potenciais sabotagens.

**Referências**

OPENAI. ChatGPT. Disponível em: <https://chat.openai.com/>. Acesso em: 03 setembro. 2025.