Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Packets Primer – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Packets Primer – Pedro Borges |
| **N° Revisão** | 1 |
| **Data de publicação** | 14/08/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/286?category=4&difficulty=2&page=2 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Pedro Borges | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Orientador |
| **Aprovação** | Sérgio Guidi Trovo | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 04/05/2025 | Produção |
| **1** | 14/08/2025 | Revisão |
| **2** | 14/08/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Análise de Pacotes, Wireshark, Forense |
| **Plataforma** | PicoCTF |
| **Área** | Blue |

**Sumário**

[Contextualização 2](#_heading=h.gjdgxs)

[Desenvolvimento 2](#_heading=h.1fob9te)

[Find](#_heading=h.3znysh7) the flag

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

O desafio Packets Primer consiste em examinar um arquivo de captura de tráfego de rede (.pcap) com o objetivo de encontrar informações que revelem a flag. Esse tipo de análise é fundamental em atividades de forense digital e segurança ofensiva, onde a inspeção de pacotes pode revelar credenciais, mensagens ou dados sensíveis transmitidos sem criptografia.

**Desenvolvimento**

**find the flag.**

Para resolver o desafio *Packets Primer*, iniciei baixando e analisando o arquivo de captura de pacotes (PCAP) fornecido. Utilizei o Wireshark, a principal ferramenta para inspeção de tráfego de rede. Ao abrir o arquivo, verifiquei a presença de múltiplos pacotes de comunicação, predominantemente utilizando os protocolos TCP e ARP.

Uma imagem contendo Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Por se tratar de um desafio para iniciantes, imaginei que a flag estaria disposta como texto claro. Com isso em mente, selecionei uma requisição TCP e com o botão direito utilizei a funcionalidade *Follow TCP Stream* para visualizar conversas completas em um formato legível. Durante a inspeção desses fluxos, identifiquei trocas de mensagens em texto claro.

Após a análise do fluxo, localizei a flag embutida no conteúdo de uma das mensagens. Ela estava no formato característico picoCTF{...}, encodada em hexadecimal, mas convertida automaticamente pelo Wireshark.

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

O desafio Packets Primer demonstrou, de forma prática, a importância da análise de tráfego de rede para identificação de informações sensíveis transmitidas em texto claro. A utilização do Wireshark facilitou a inspeção e interpretação dos dados capturados, permitindo a extração eficiente da flag. A abordagem de seguir fluxos TCP e buscar mensagens legíveis se mostrou eficaz, principalmente considerando a simplicidade do desafio voltado para iniciantes.