ATIVIDADE ORIENTADA AO ENSINO

Relatório simplificado dos tópicos estudados

Acadêmico: Matheus Clisman Mariano da Silva

RGA: 202119050055

Professor: Carlos Alberto da Silva

1 Introdução

Este relatório apresenta, de forma simples e direta, os tópicos estudados durante a atividade orientada ao ensino. As imagens utilizadas neste trabalho foram retiradas das plataformas TryHackMe (THM) e LetsDefend, e foram mantidas apenas como evidências do que foi feito ao longo dos estudos.

2 Tópicos estudados

Durante a atividade, estudei reconhecimento de rede de computadores com Nmap, análise de requisições com Burp Suite, exploração de vulnerabilidades como XSS e IDOR, quebra de hash com John the Ripper e análise de alertas e logs em ambiente de monitoramento (Usando ferramentas como Splunk). Também tive contato com tarefas práticas em laboratórios da THM e da LetsDefend, o que ajudou a fixar o conteúdo de maneira mais concreta.

3 Evidências das atividades

3.1 TryHackMe - Reconhecimento de rede

Nesta etapa, estudei a identificação de serviços e portas abertas com Nmap em um laboratório da THM.

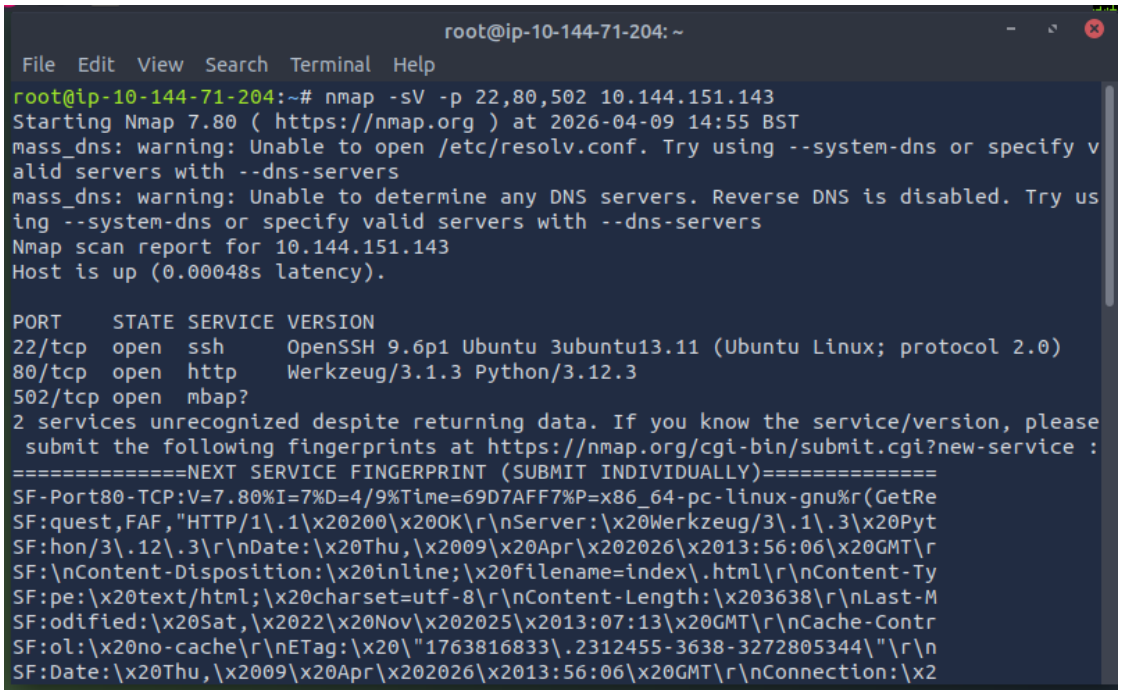

Figura 1: Evidência de reconhecimento de rede na plataforma TryHackMe

3.2 TryHackMe - Análise de requisições

Também estudei a utilização do Burp Suite para interceptar e analisar requisições HTTP em cenários de teste.

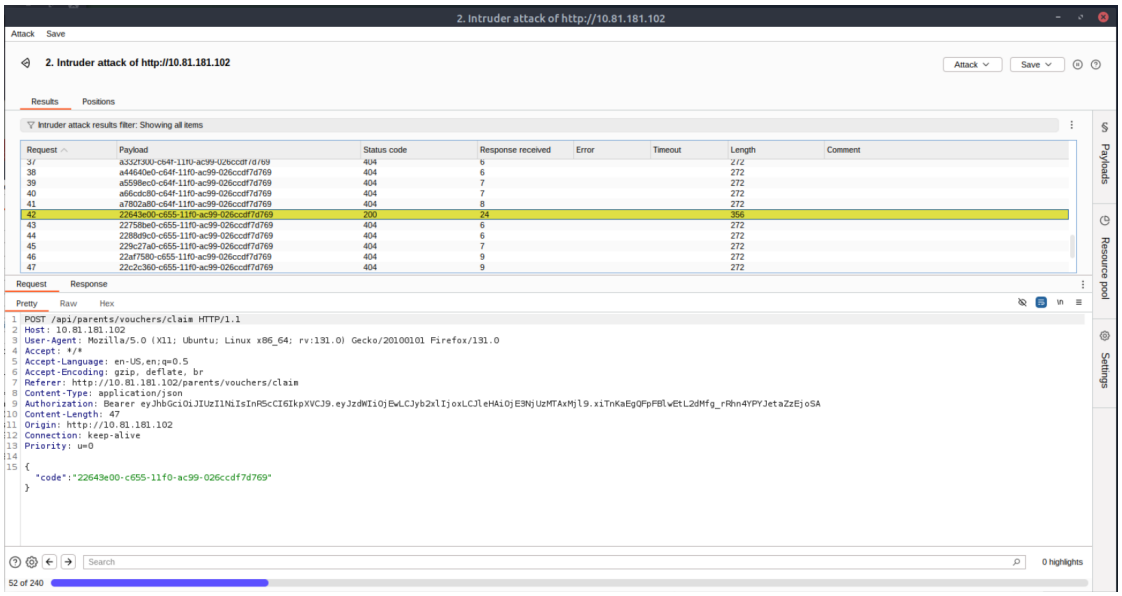

Figura 2: Evidência de análise de requisições na plataforma TryHackMe usando Burp Suite

3.3 TryHackMe - XSS e IDOR

Nos laboratórios da THM, estudei testes relacionados a XSS e IDOR, com uso de diferentes ferramentas de apoio para análise e validação das requisições.

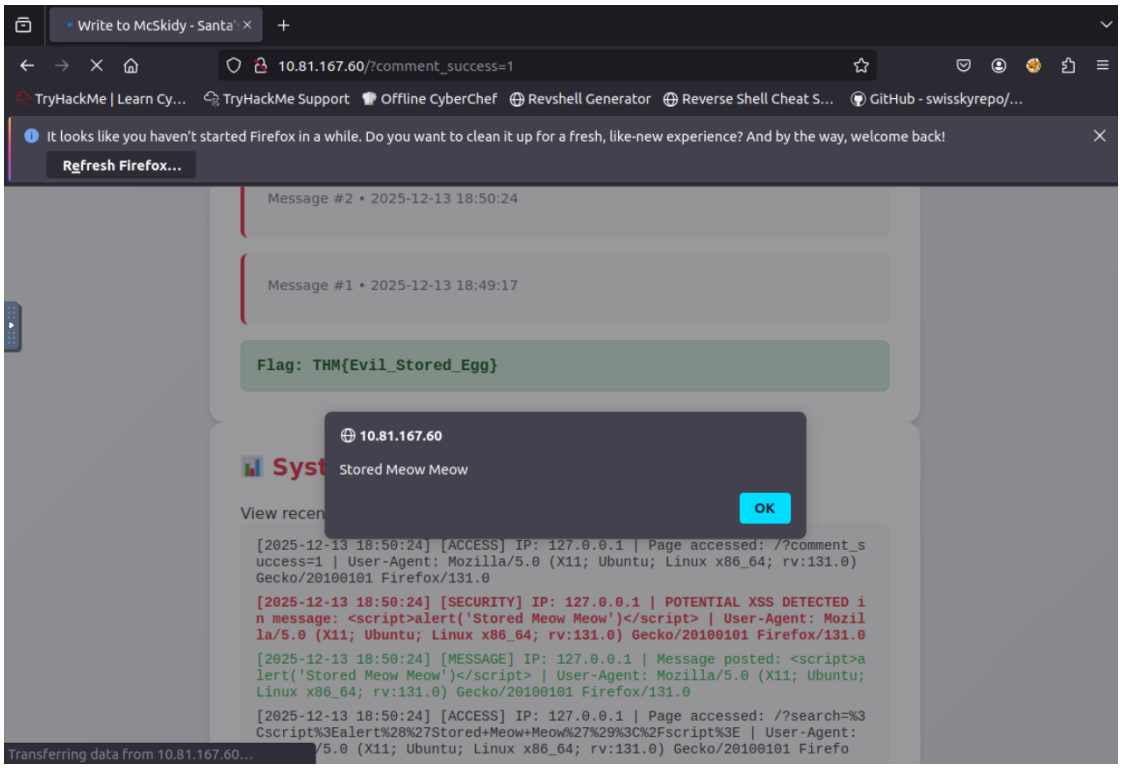

Figura 3: Evidência de estudo de XSS na plataforma TryHackMe

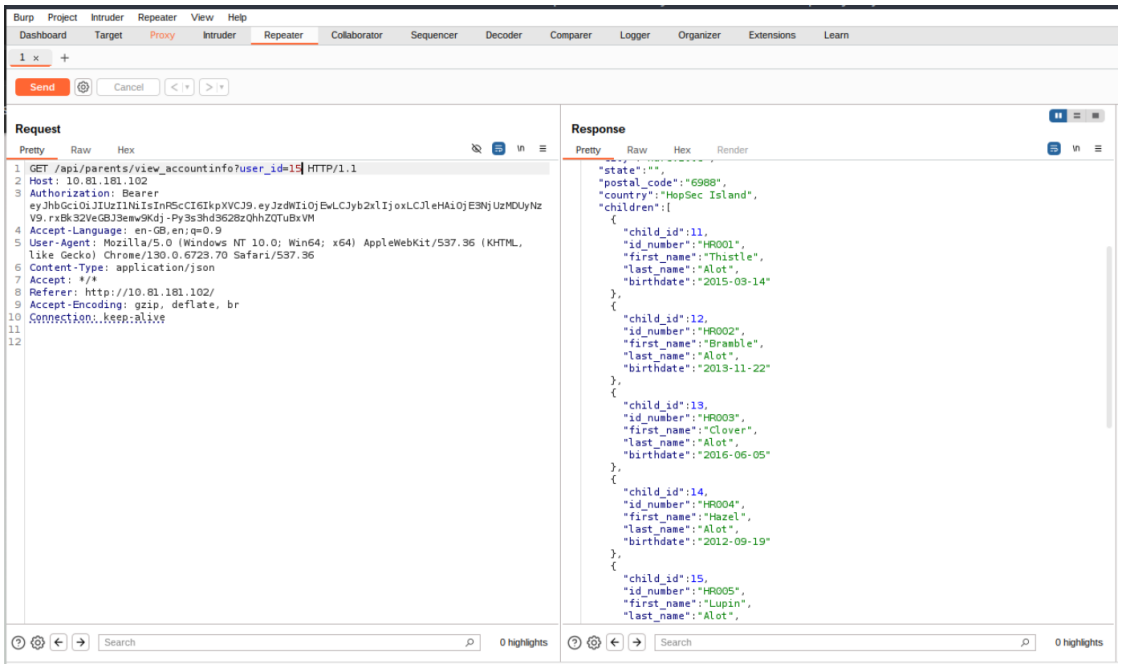

Figura 4: Evidência de estudo de IDOR na plataforma TryHackMe usando Burp Suite

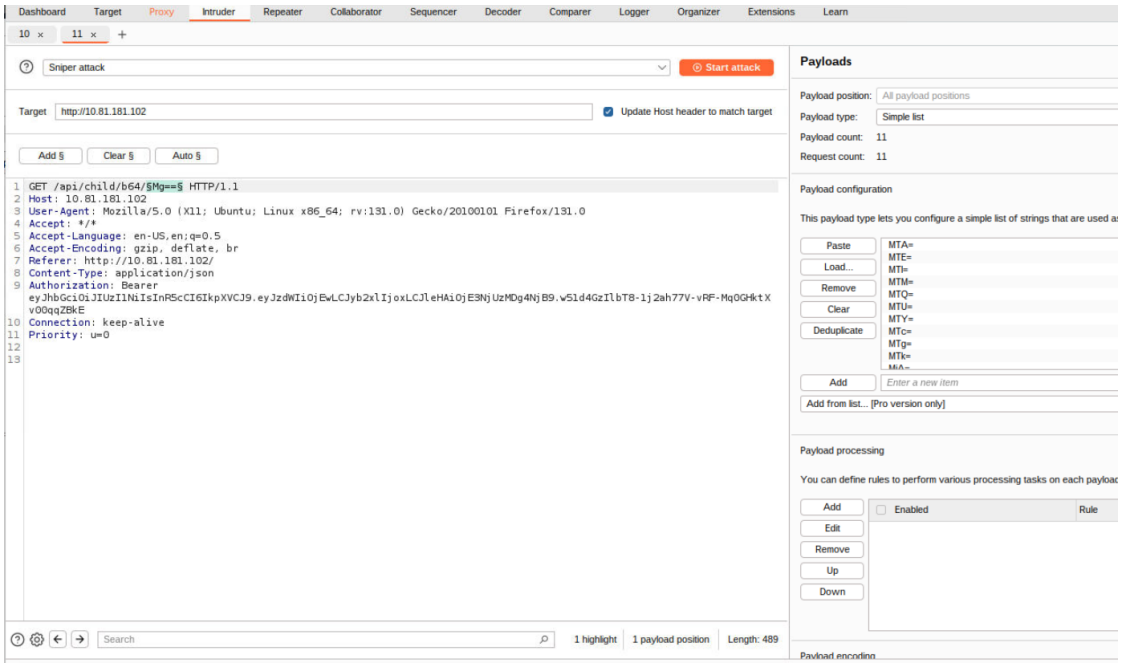

Figura 5: Evidência de automação de testes com Burp Intruder na plataforma TryHackMe

3.4 TryHackMe - Quebra de hash

Outro tópico estudado foi a quebra de hash com John the Ripper, aplicando o conteúdo em um laboratório prático da THM.

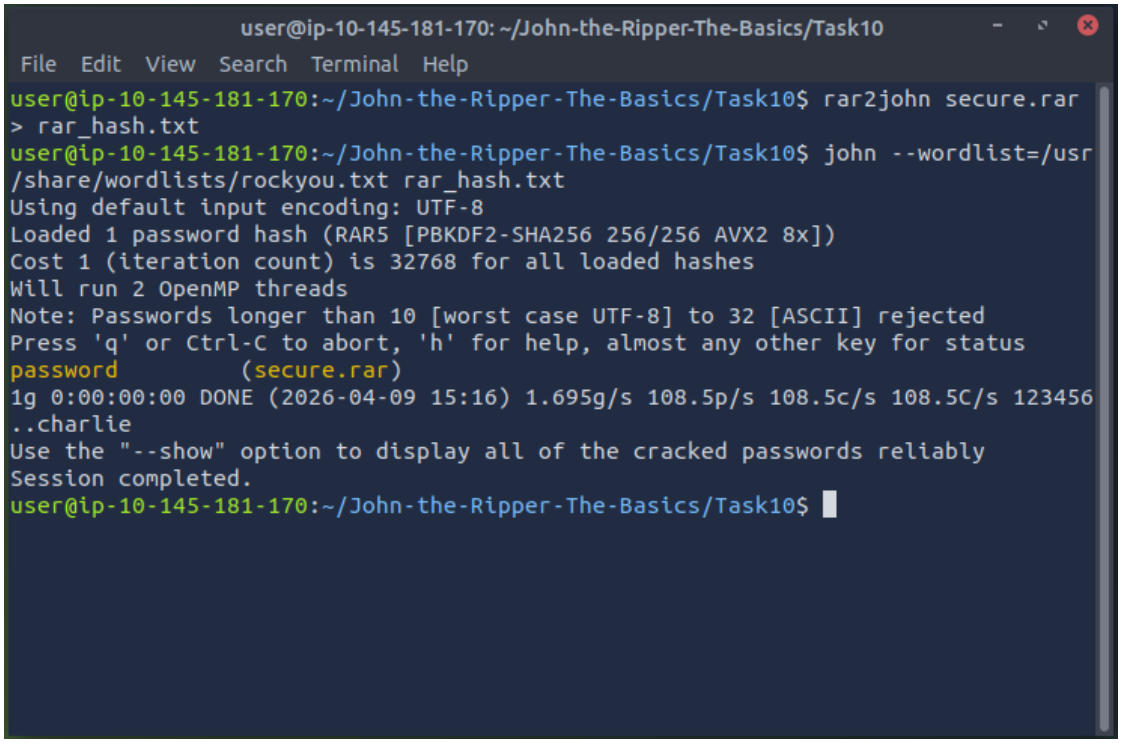

Figura 6: Evidência de quebra de hash na plataforma TryHackMe

3.5 LetsDefend - Análise de alertas e logs

Na LetsDefend, estudei a análise de alertas, leitura de eventos e observação de logs para entender melhor a rotina de monitoramento em segurança.

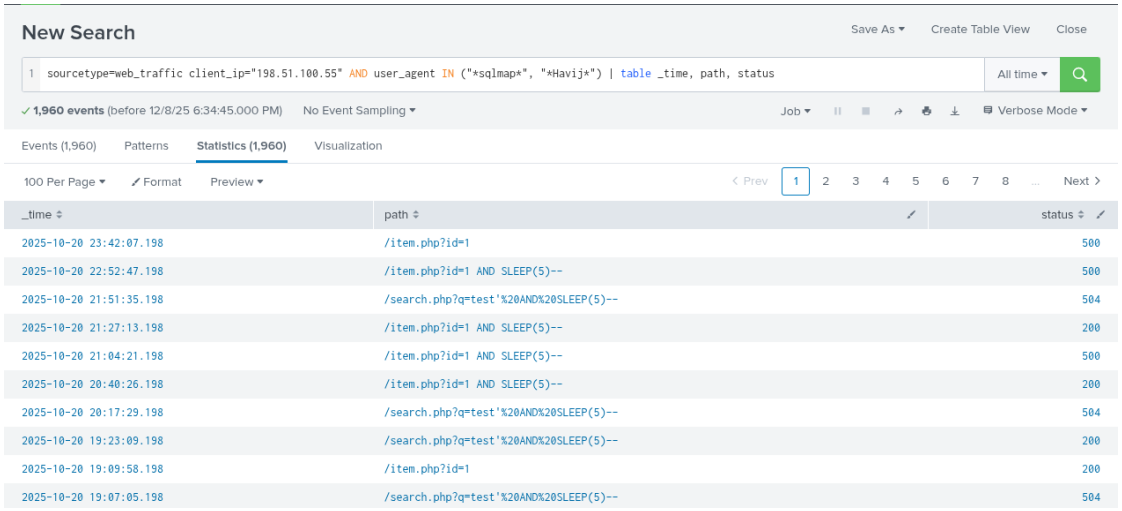

Figura 7: Evidência de análise na plataforma LetsDefend usando Splunk

4 Conclusão

Ao longo da atividade, foi possível estudar diferentes tópicos de forma prática e objetiva, com apoio das plataformas TryHackMe e LetsDefend. Eu desenvolvi novas habilidades em cima dos topicos estudados, principalmente na análise de ambientes, no uso das ferramentas apresentadas e na interpretação das evidências obtidas durante os laboratórios.