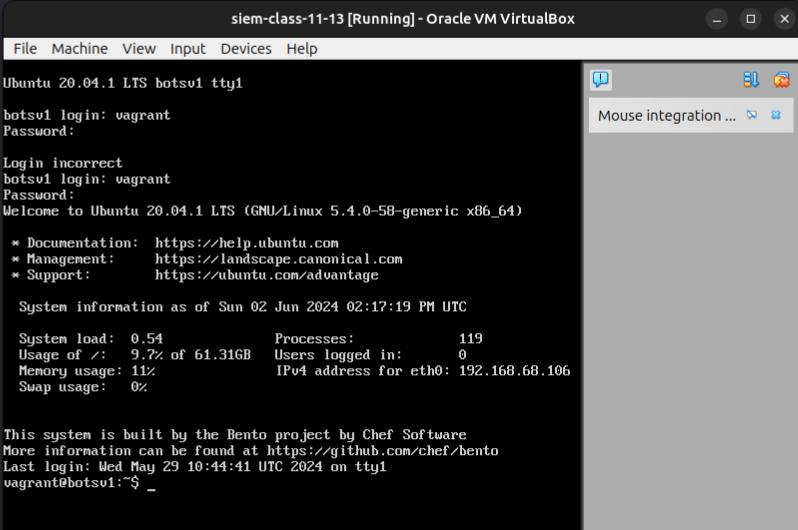
Hélio Ferreira 28/05/2024

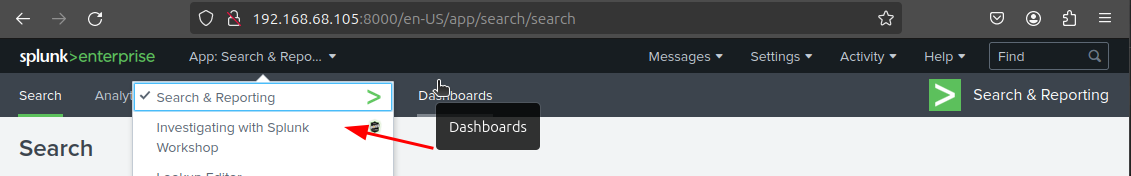
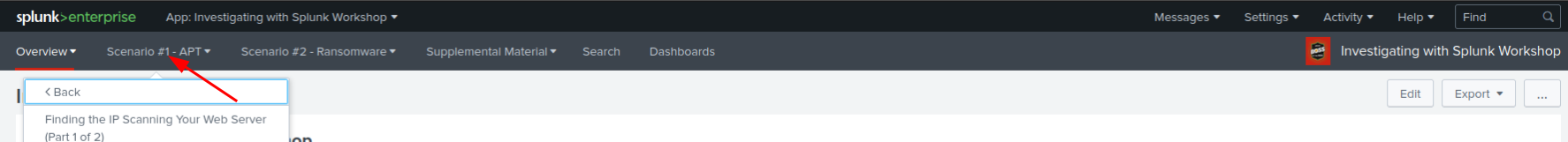
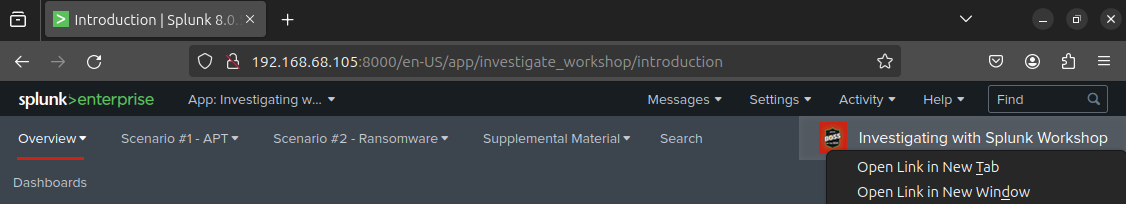
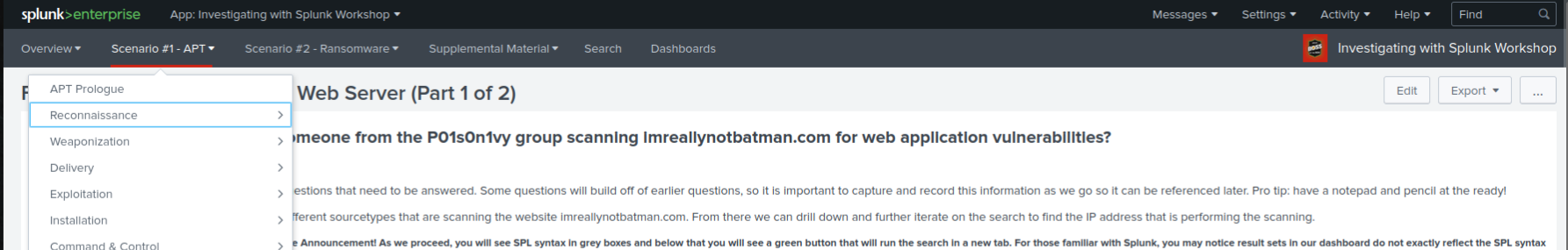
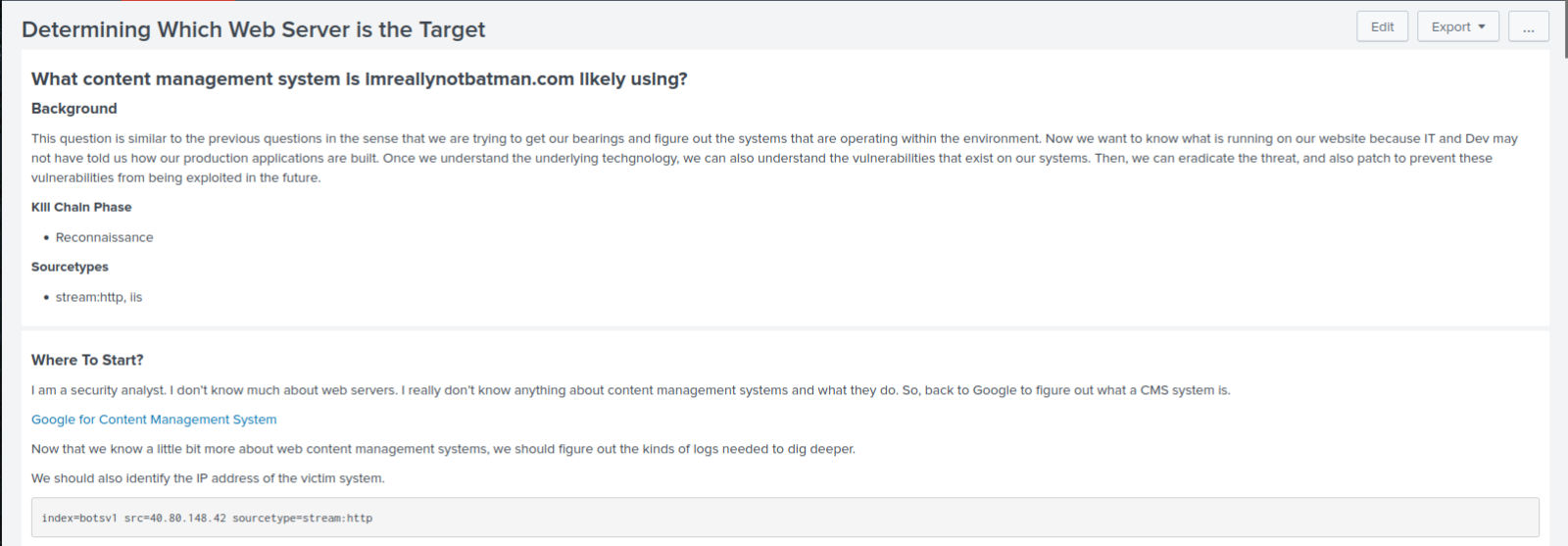
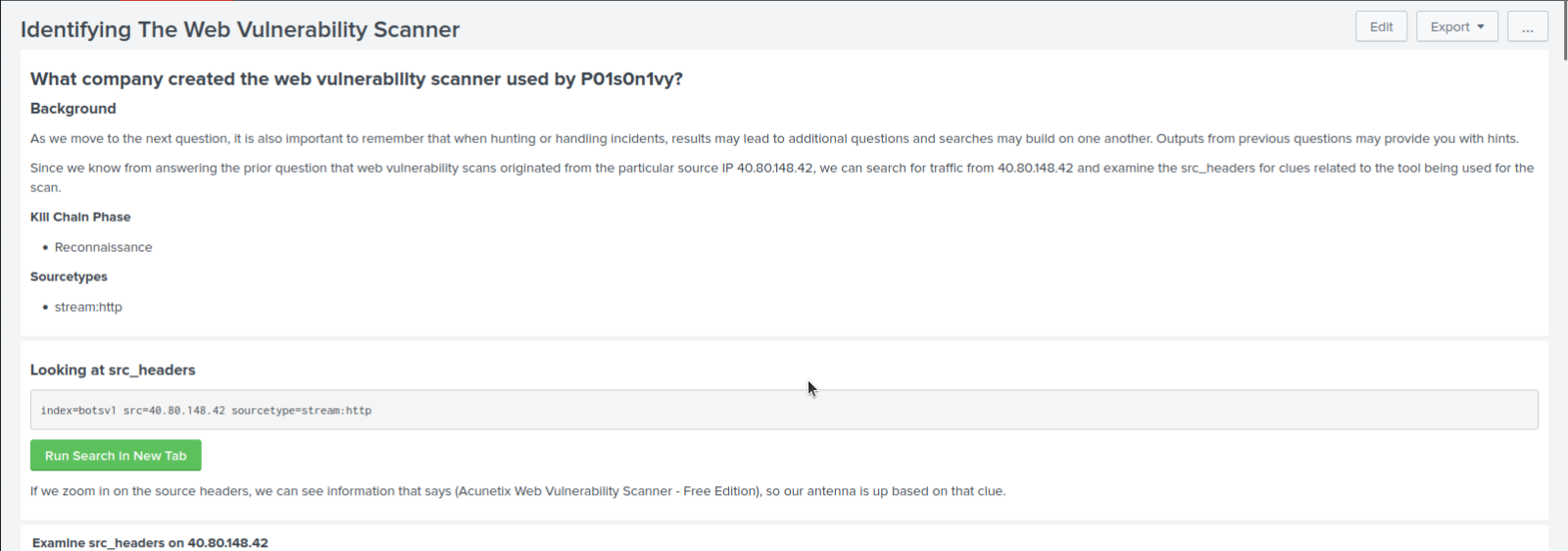
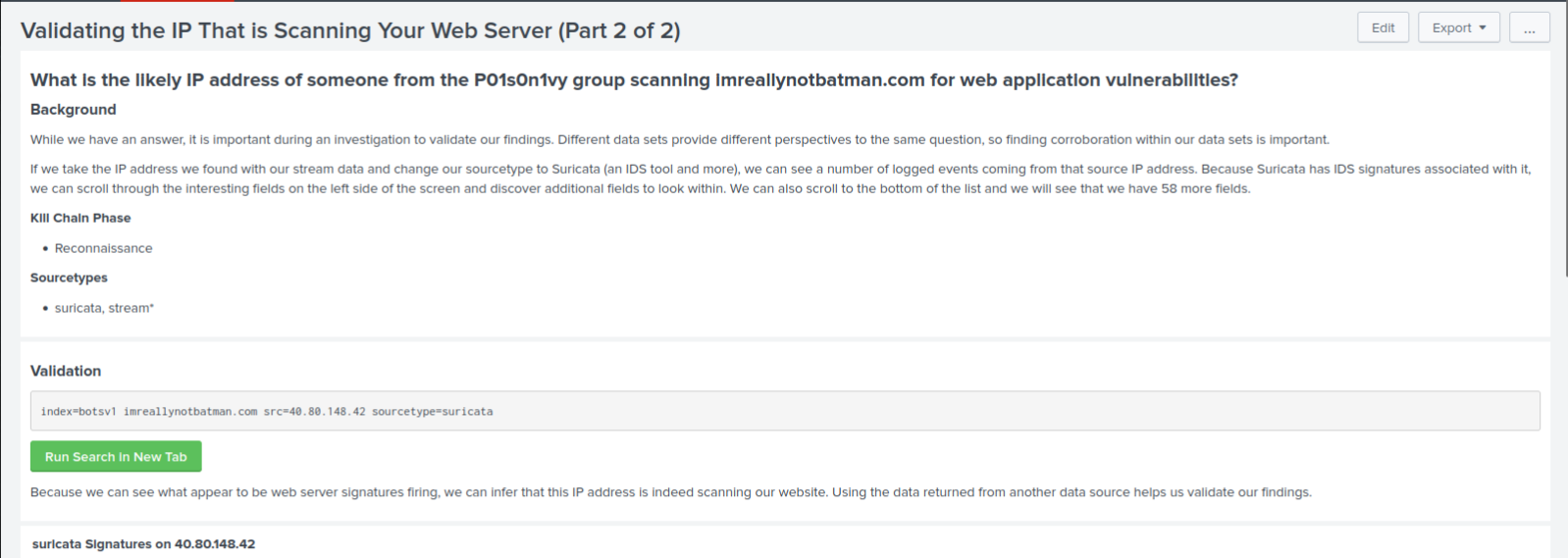
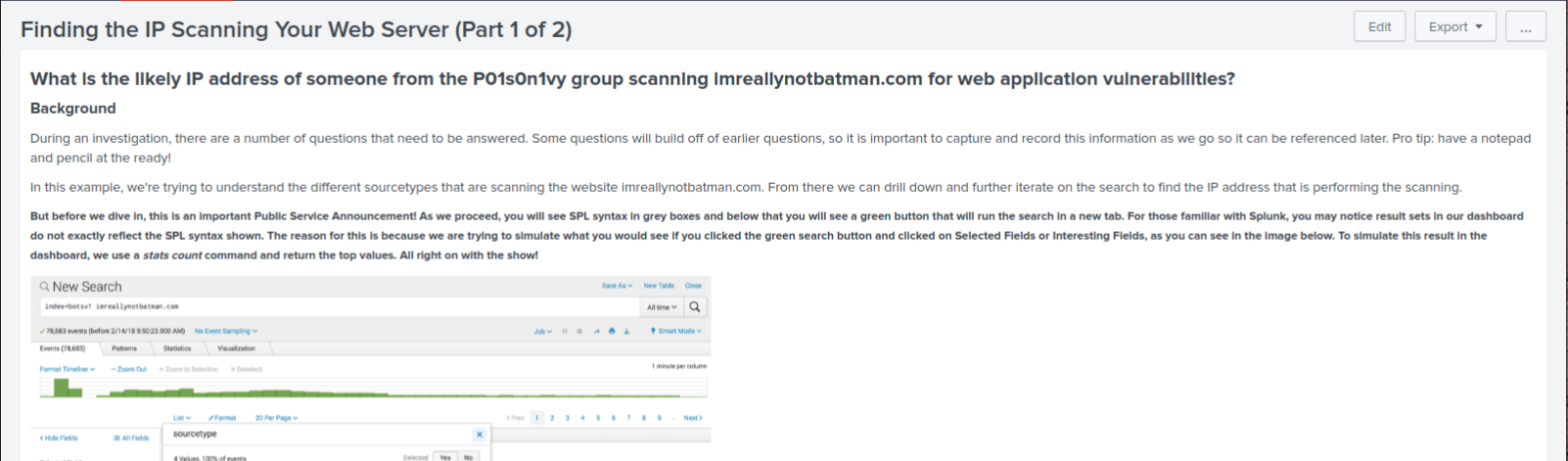
# **Log Analysis with Splunk**

### **Part 1: Staging**

* Log into the same Splunk server you used yesterday and run the “Investigating with Splunk Workshop” app to access the lab instructions. You’ll want to open a separate browser tab for querying data using the Search and Reporting app on this same Splunk server.  
  

### **Part 2: BOTSv1**

Boss of the SOC is a blue-team CTF workshop that lets participants practice hunting and analysis skills. You will use Splunk and other tools to answer questions about security incidents that have occurred in a realistic but fictitious enterprise environment. It’s designed to emulate how real security incidents look in Splunk and the type of questions analysts must answer. The idea is to recreate the life of a security analyst facing down an adversary at all stages of an attack.

* Run the Splunk app, Investigating with Splunk Workshop.
* You’ll now be working on completing the following sections in Boss of the SOC (BOTS) Version 1, Scenario #1 - APT:  
    
  
  + Reconnaissance  
      
      
    
  + Exploitation