

Boss of the SOC is a blue-team CTF that helps you enhance your hunting and analysis skills. You will use Splunk and other tools to answer a variety of 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 have to answer. The objective is to recreate the life of a security analyst facing down an adversary at all stages of an attack.

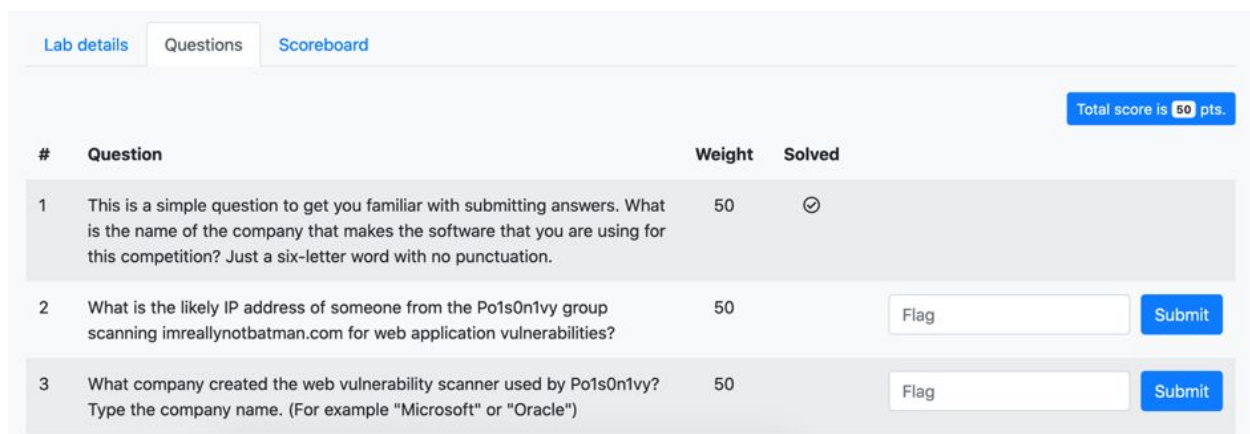
Note: All the information you need to answer each question is present within the question itself. You just need to figure out how to create the proper Splunk search query that will get you the information you want.

Rules:

1. Each question will have a base score. The harder the question, the higher the base score. If you answer the question correctly, you will receive the base score for that question.
2. Don't be evil.

To start playing, click on **"Start"**. Once started, you will instantly be provided with lab access URL and credentials which will be used to access Splunk.

Also, the **Questions** section will be active and you can start submitting answers.



The screenshot shows a web interface with three tabs: "Lab details", "Questions", and "Scoreboard". The "Questions" tab is active. In the top right corner, a blue box displays "Total score is 50 pts.". Below this is a table with the following columns: "#", "Question", "Weight", and "Solved".

#	Question	Weight	Solved
1	This is a simple question to get you familiar with submitting answers. What is the name of the company that makes the software that you are using for this competition? Just a six-letter word with no punctuation.	50	☑
2	What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?	50	<input type="text" value="Flag"/> <input type="button" value="Submit"/>
3	What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name. (For example "Microsoft" or "Oracle")	50	<input type="text" value="Flag"/> <input type="button" value="Submit"/>

To get started, you will need to:

- Analyze data and look for answers: Click on **"Search Server URL"** to open Splunk search page. This is where you will spend all of your time trying to find answers. Select

"Search and Reporting" and type the following in the search bar **earliest=0** This will select the right data set and time frame for your search queries.

- Click "**No Event Sampling**" and select "**1: 100**".... this will display only a sample of each search result to speed up the process.

The screenshot shows the Splunk Search & Reporting interface. At the top, the search bar contains the query `earliest=0`, with a red arrow labeled '1' pointing to it. Below the search bar, the results summary shows '613,832 of 594,264 events matched' and 'Sampling 1: 100', with a red arrow labeled '2' pointing to the sampling rate. On the left side, the 'Selected Fields' section is expanded, showing fields like `host`, `source`, and `sourcetype`, with a red arrow labeled '3' pointing to it. The main content area displays a list of search results, including a sample event from 8/31/17 at 2:53:06.470 AM with a detailed JSON payload.

- To get a quick idea of what you are dealing with, check the "**Selected Fields**" section at the left side of the page and you will be able to see number of hosts and available log sources.

How Can I Prepare?

- Check out our "[Hunting With Splunk](#)" blog series. More than anything else, mastering the topics covered in this series will help you answer more questions faster
- Take advantage of [Free Splunk Fundamentals 1 Training](#)