Black Sabre Response

IRTx Closure Report

# Overview

The task of the IRTx was to test the blue teams runbooks against the opposing red team playbooks and test the IRP. The red team would attack the network following their books while the goal of the blue team is to detect any attempted un/successful attacks. There was a time limit of 2 hours for the red team to attack and finish their playbooks.

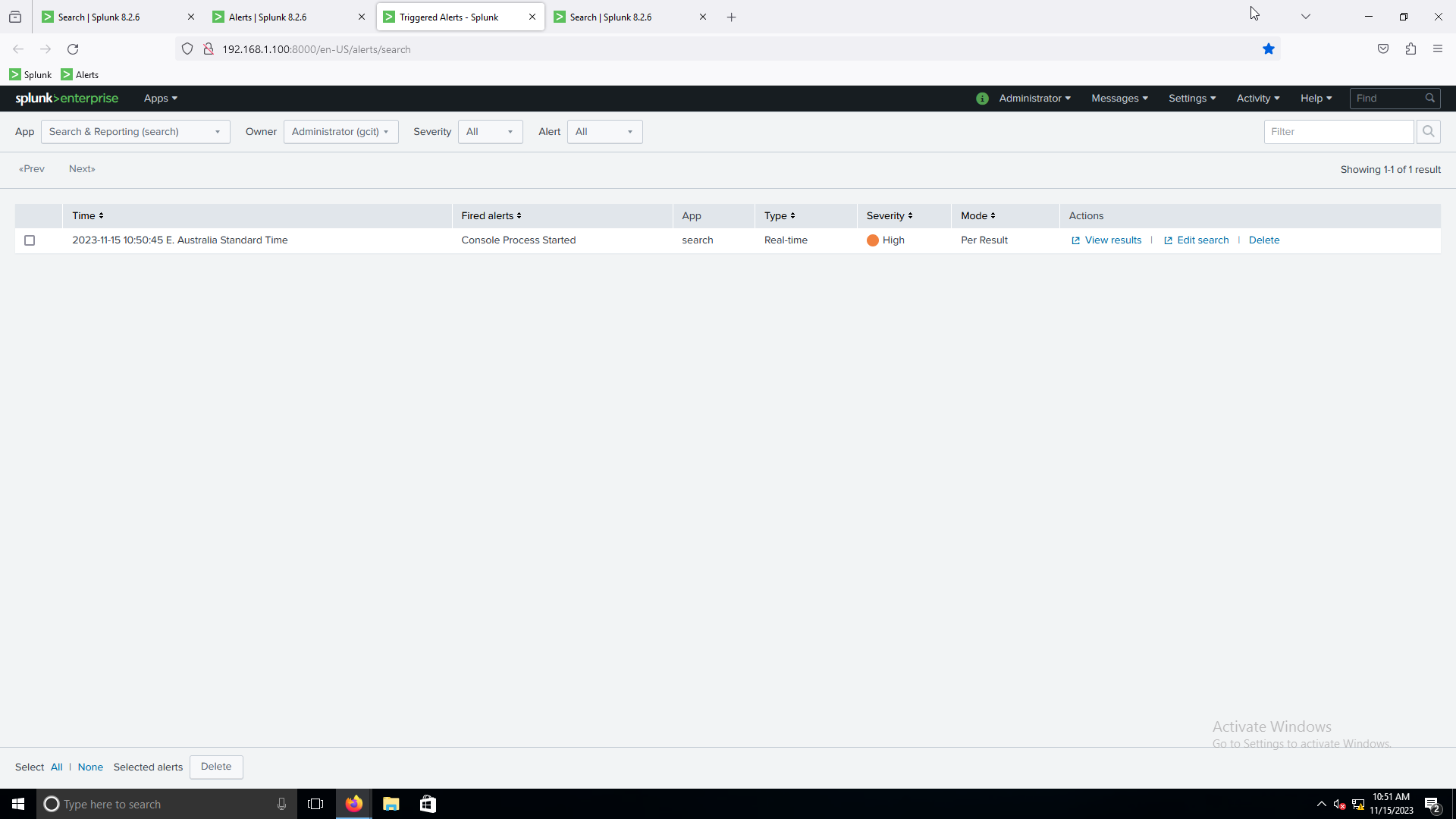
Both teams successfully completed their tasks with the red team successfully completing their book and the blue successfully detecting all incoming attacks.

# Strategy Review

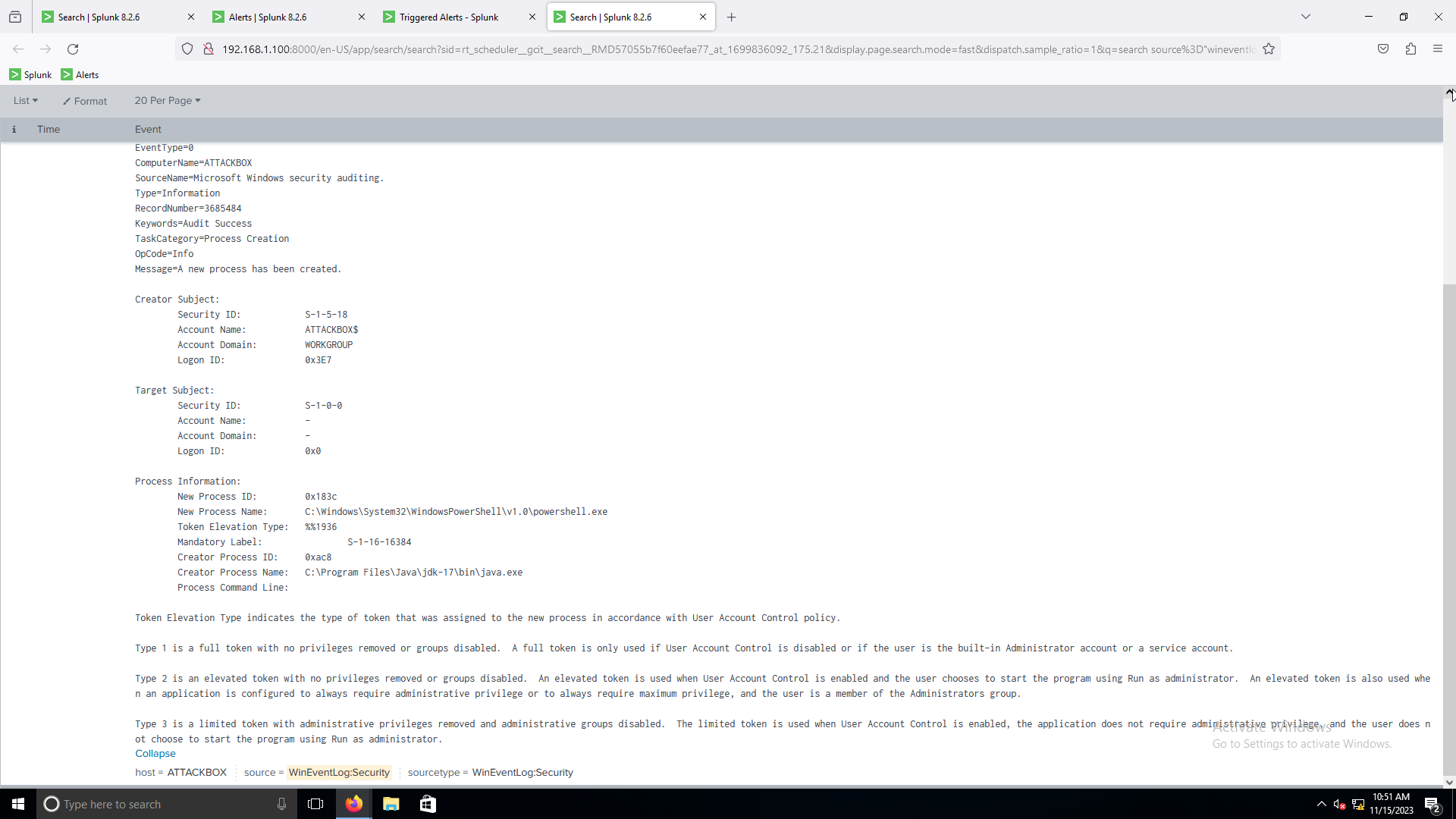
## Blue Team strategy

The strategy of the blue team was to setup alerts in splunk for the attacks the red will use. These alerts should cover and detect exactly what the red team is doing according the correct log. During the exercise, the blue team will see the alert and from there open the alert in the search tab to confirm the authenticity of the attack and whether it is a false positive or not

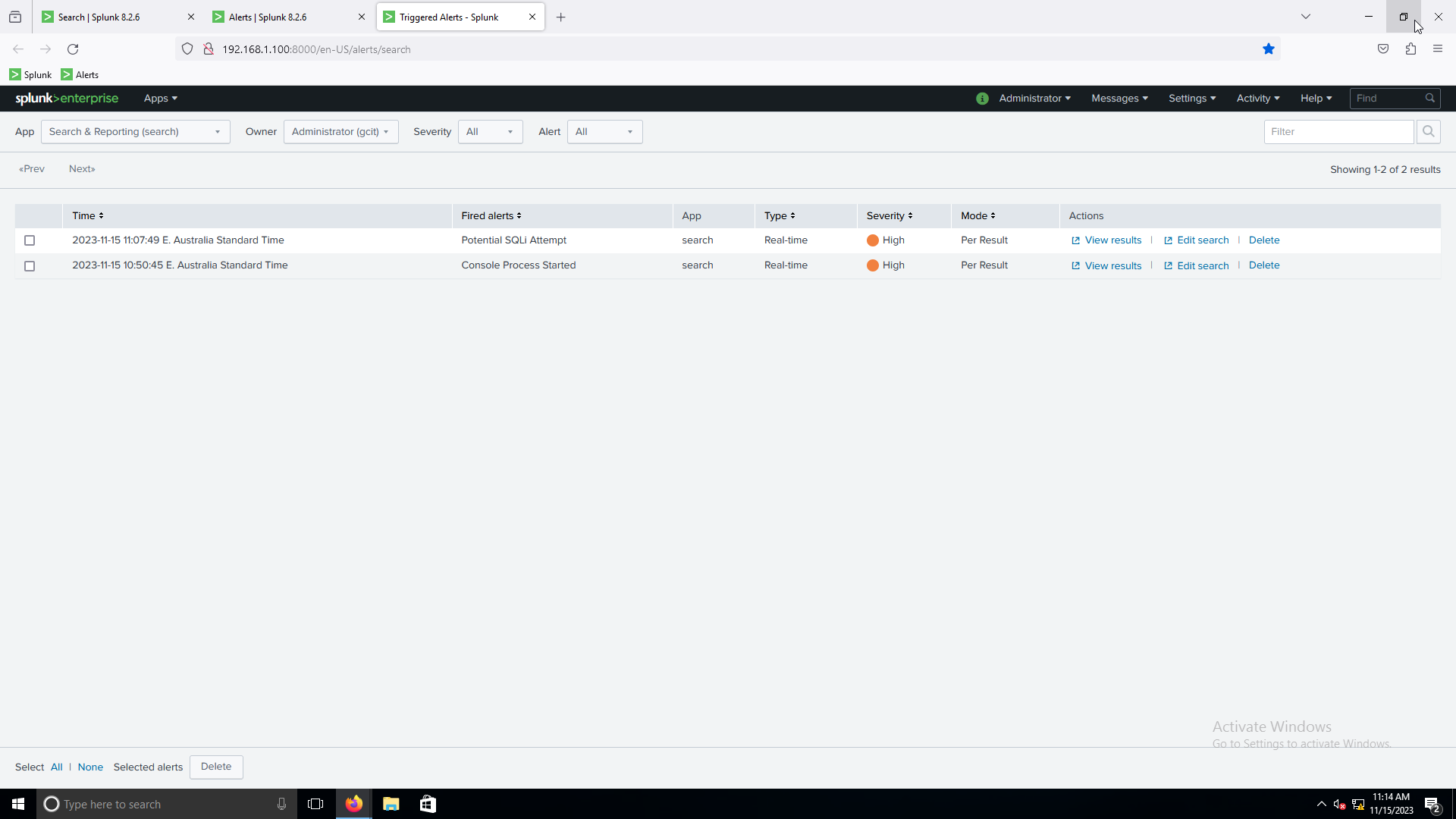
## Summary of Results

The first attack was a reverse shell via jenkins. Blue team setup an alert to detect any console processes starting. The alert successfully triggered when the red team got the reverse shell.

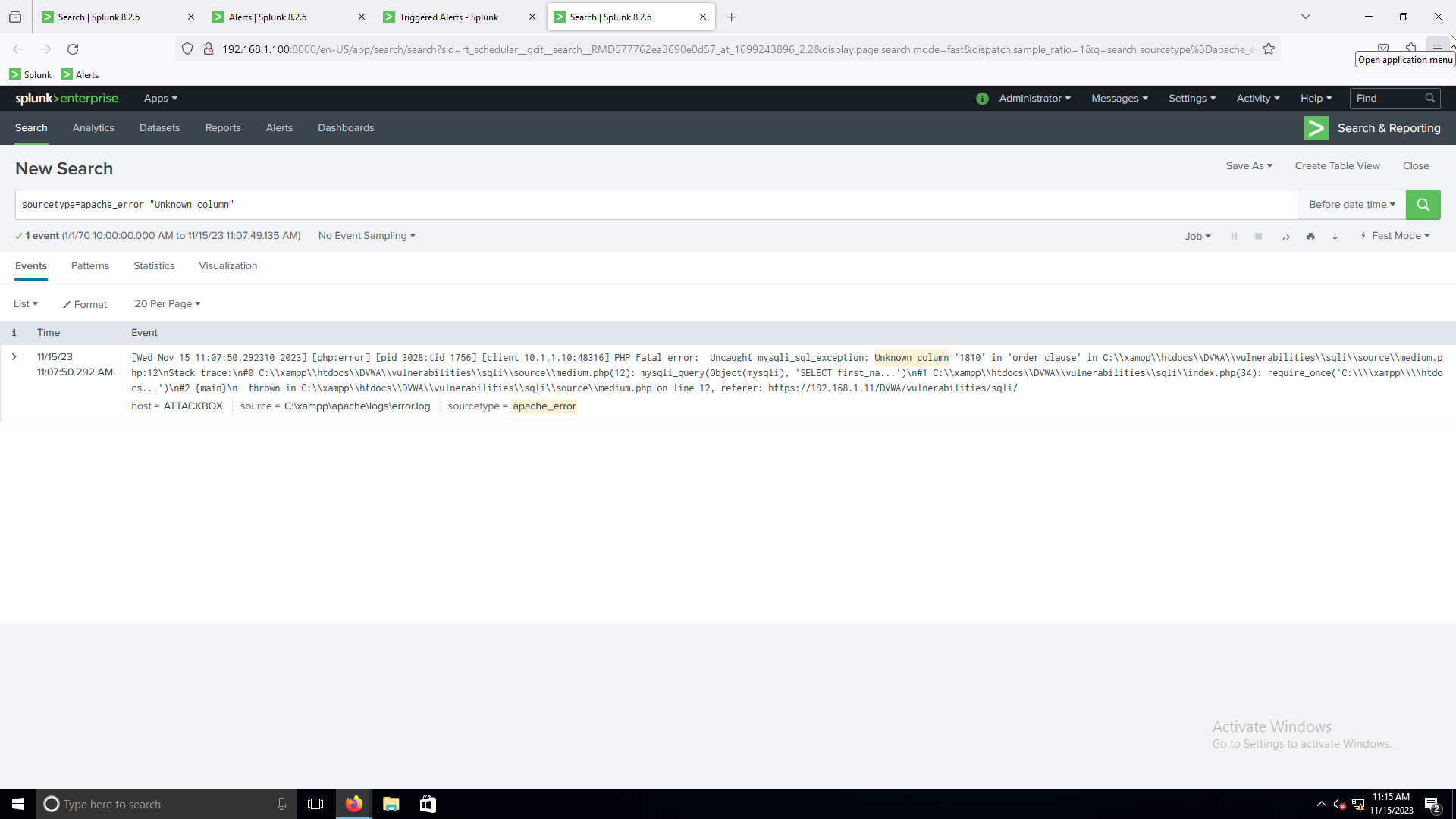
Deep dive into alert to confirm attack



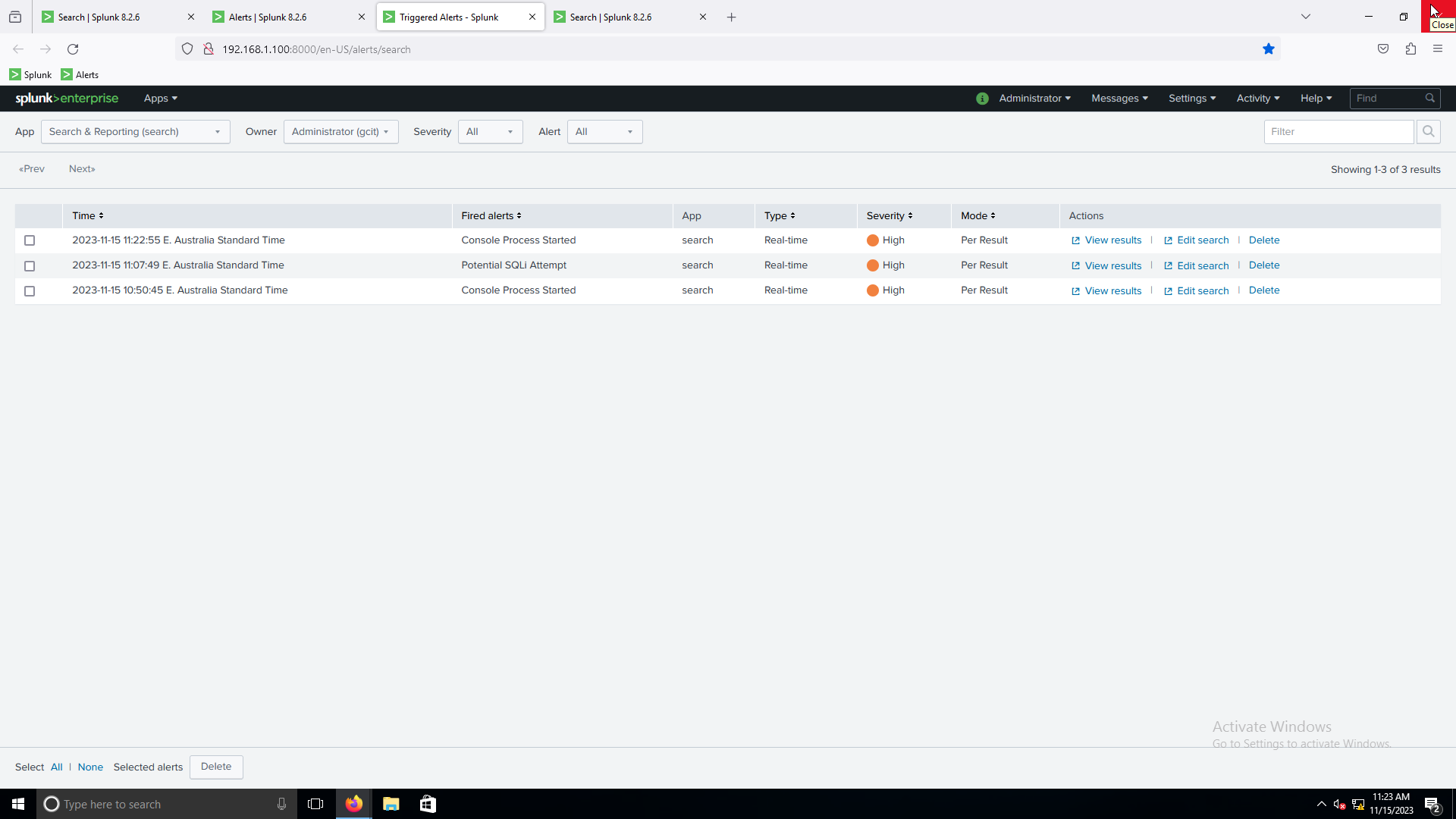
The second attack was sqli. Blue team successfully detected the potential SQLi.

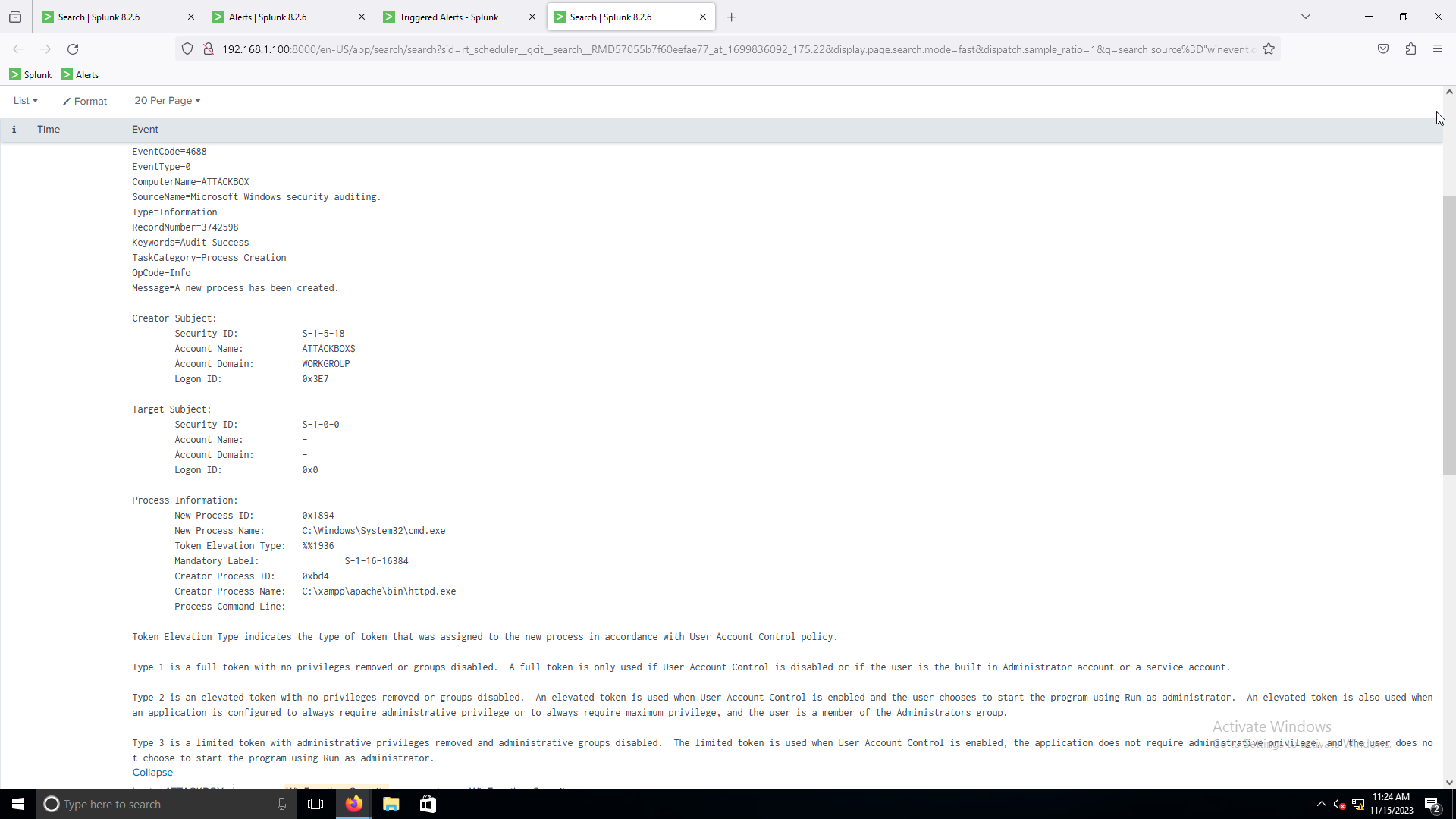


Deep dive



The last attack was a file upload vulnerability

Deep Dive



## Strategy effectiveness

As per the results above, the blue team strategy was extremely effective in detecting all attacks done by the red team. This would allow the blue team to follow up with remediation/incident response in a very timely manner reducing the potential impact the attackers could have.

## Communication effectiveness

The communication between the teams was effective and meant everyone knew what was happening and everyone got updates as soon as they happened. This also includes the stakeholder being kept up-to-date with the results of both the red and blue teams.

# Lessons Learnt

## What went right

1. The blue team successfully detected all attacks with minutes of the attackers running them.
2. The red team attacks were all successful in achieving the desired results whether it be database dumping or reverse shells.
3. Communication between all parties was effective and precise.

## What went wrong

1. Red runbook was too vague making it a bit harder to complete attacks
2. MSF module for jenkins console didn’t work (although was good opportunity to show automated methods won’t always work).
3. Red team box didn’t have internet access so the code for reverse shells had to be kept on the desktop.

## Improvements

1. Make the red runbook more clear on how to run the attacks and less vague.
2. Give the red team box internet access so the attacker have to find the reverse shell code to make it more realistic.
3. Find attack where the MSF module works.

## Appendix

|  |  |
| --- | --- |
| **Section** | **Author** |
| **Closure Report** | Dylan and Syed |