Project Week: Building a Security Monitoring Environment

Cybersecurity

Project 3


WELCOME

For your third project, you will use the skills that you've learned in the Defensive Security unit to design a custom monitoring environment to protect a fictional organization.


Recap

Day 1 Recap

Since VSI heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business, you were tasked with using Splunk to develop a monitoring environment.

This environment can protect against potential attacks on VSI's systems and applications.

(source)

Recap

In the last class, you developed a monitoring environment by:

- Loading and analyzing Windows logs.
- Creating reports, alerts, and dashboards for the Windows logs.
- Loading and analyzing Apache logs.
- Creating reports, alerts, and dashboards for the Apache logs.
- Installing add-on Splunk applications for additional monitoring.

Today’s Class

The rest of today’s class will proceed as follows:

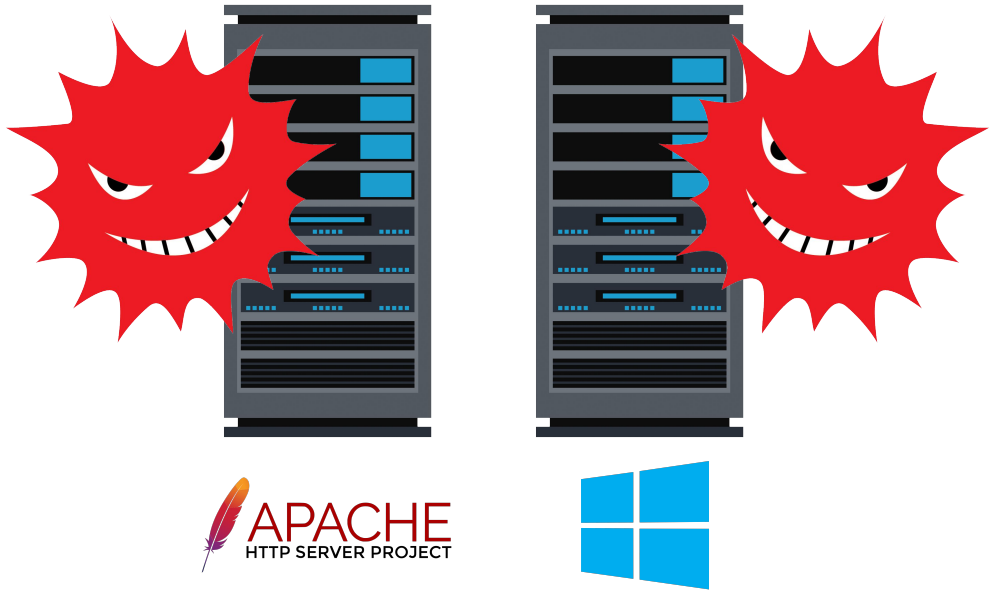
- Introduction to today’s project scenario
- Overview of daily tasks
- Preview of presentations for next class
- Project work

Day 2
Overview

Day 2 Overview

You have just been notified by your manager that VSI recently experienced several cyberattacks, likely from their adversary JobeCorp. Unfortunately, this attack took down several of VSI's systems.

- Fortunately, you have just set up several monitoring solutions to help VSI quickly identify what was attacked.
- The attack that occurred targeted several systems — specifically, the Windows and Apache servers, which you are fortunately monitoring.
- Management has provided you with more logs from those same servers. These new logs cover the time period during which the attack occurred.



Day 2 Overview

You are now tasked with analyzing these “attack logs” with your monitoring solution to determine the efficacy of your solution.

Additionally, your findings will help VSI create any further mitigation strategies that are necessary.

Lastly, you will create a presentation that showcases your monitoring solution and your findings to senior management.

Today's Steps

01 Load Windows attack logs.

02 Analyze Windows attack logs.

03 Load Apache attack logs.

04 Analyze Apache attack logs.

05 Create project presentations.

Step 1 Load Windows Attack Logs

First, you will receive a set of “attack logs” from the Windows servers that run VSI’s back-end systems.

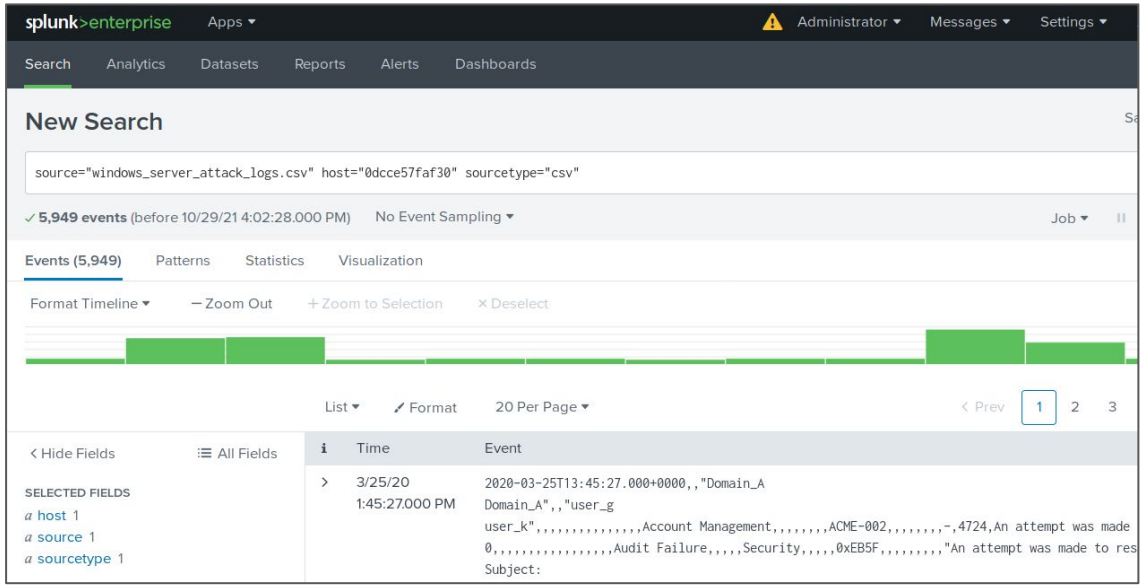
These logs were captured during the time when the attack occurred.

The activity guide will provide steps for loading and configuring these new logs.

```
sysadmin@UbuntuDesktop:/splunk/logs/Week-2-Day-3-Logs$ ls -ltr
total 38484
-rwxrwxrwx 1 root root 19475049 Jun 25  2020 windows_server_attack_logs.csv
-rwxrwxrwx 1 root root  2398733 Jun 25  2020 apache_logs.txt
-rwxrwxrwx 1 root root  1021447 Jun 25  2020 apache_attack_logs.txt
```

Step 2 Analyze Windows Attack Logs

Then, you will analyze the Windows attack logs to determine how effective your monitoring solution was or wasn't.



Step 3 Load Apache Attack Logs

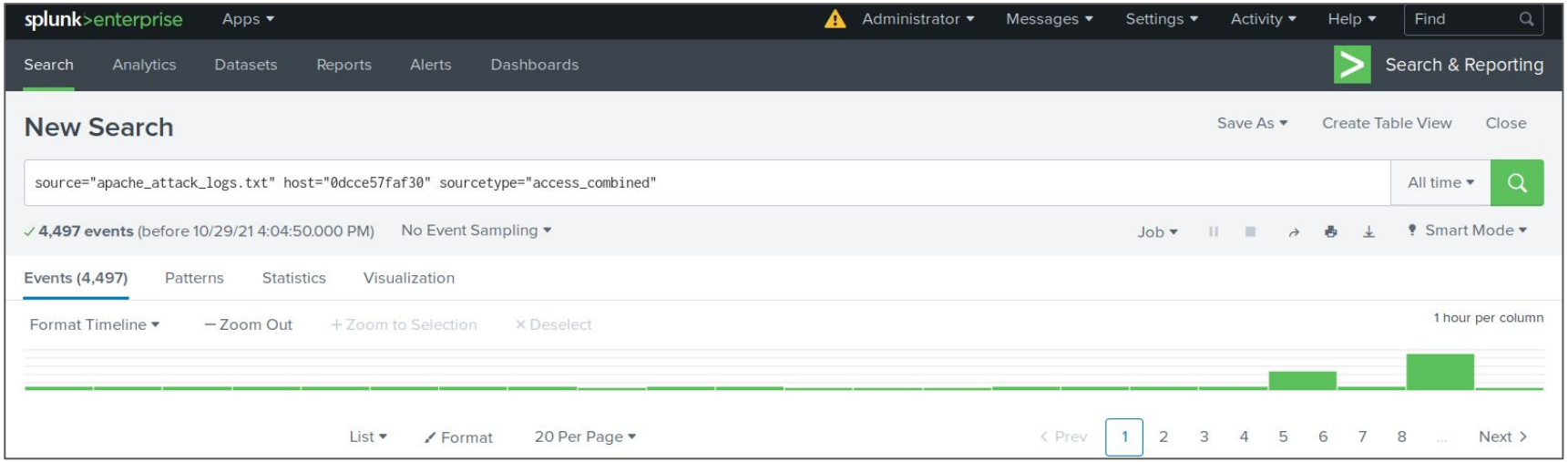
You will also receive a set of “attack logs” from the Apache servers that run VSI’s back-end systems.

- These logs were captured during the time when the attack occurred.
- The activity guide will provide steps for loading and configuring these new logs.

```
sysadmin@UbuntuDesktop:/splunk/logs/Week-2-Day-3-Logs$ ls -ltr
total 38484
-rwxrwxrwx 1 root root 19475049 Jun 25  2020 windows_server_attack_logs.csv
-rwxrwxrwx 1 root root  2398733 Jun 25  2020 apache_logs.txt
-rwxrwxrwx 1 root root  1021447 Jun 25  2020 apache_attack_logs.txt
```

Step 4 Analyze Apache Attack Logs

Then you will analyze the Apache attack logs to determine how effective your monitoring solution was or wasn't.



Step 5

Start Creating Project Presentations

In today's final step, you will begin preparing slides for a presentation of your work this week. You will present in groups on Day 3 of this project.

A framework for the slides and instructions will be provided to assist in the creation of the presentation.

Next Class

You will present.

After you complete today's activities, begin working on your presentations.

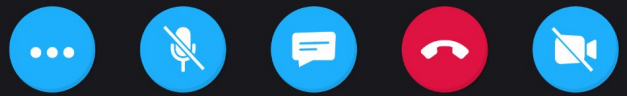
Project Day 3 Schedule:

First 30 minutes:

You will work in groups to finalize your project presentations.

Remaining 2 hours:

Groups will present their project presentations.



Day 3 Presentations

- Each group will have a 15-minute time slot for their presentation. Plan for a max of 12 minutes presenting, followed by 3 minutes of Q&A.
- Groups can choose to have 1 presenter for the whole group, or have the group split up the presentation among group members.
- Work with your group to prepare the presentation, but every student must submit a complete presentation as a deliverable (even if it is the same as other group members').
- Use the framework provided for the presentation for general guidance, but feel free to enhance or adjust your presentation as your team sees fit.

Activity: Attacks Incoming!

In this project, you will analyze “attack logs” and determine how effective your monitoring solution was or wasn’t.

Suggested Time:

To End of Class

Project Work Time

Questions?


The End