



Cybersecurity

Day 2 Activity Guide

Monitoring and Analyzing Attacks

Today, you will determine whether your monitoring solution protected VSI. Specifically, you will:

1. **Load Windows attack logs.**
2. **Analyze Windows attack logs.**
3. **Load Apache attack logs.**
4. **Analyze Apache attack logs.**
5. **Create project presentations.**

Resources

- [Splunkbase](#)
- [Splunk Documentation](#)
- [Splunk Add-Ons Guide](#)

Getting Started / Prerequisites

You will use your local Vagrant virtual machine for this week's activities.

- This week's classes will use the same Splunk Docker container to run Splunk from inside the local virtual machine that was used during the Splunk lessons. In the `/splunk` directory inside the virtual machine, you will find a `splunk.sh` script that can be run to start and stop the container as needed.
- If needed, refer back to the Module 19 guide to configure Splunk on your VM.

- Once the container is running, Splunk can be accessed at <http://localhost:8000> on the virtual machine.

Use the following credentials:

- **Username:** admin
- **Password:** cybersecurity

Instructions

Scenario

Welcome to Day 2 of your Defensive Security project!

- 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.
- You are now tasked with analyzing these “attack logs” with your monitoring solution to determine the efficacy of your solution.
 - Additionally, you will complete the following review questions during your analysis: [Project 3 Review Questions](#).
- Lastly, you will create a presentation that showcases your monitoring solution and your findings to senior management.


You've been provided the following new logs:

- **Windows Server Attack Logs**
- **Apache Server Attack Logs**

Follow the steps below to complete your Day 2 tasks.

Part 1: Load Windows Attack Logs

In this first part, you will upload Windows attack logs into your Splunk environment. To do so, complete the following steps:

1. Select the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
 - Click “Select File.”
 - Select the `windows_server_attack_logs.csv` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
 - Click the green “Next” button on the top right.
3. You will be brought to the “Set Source Type” page.
 - You don't need to change any configurations on this page.
 - Select “Next” again.
4. You'll be brought to the “Input Settings” page.
 - This page contains optional settings for how the data is input.
 - In the “Host” field value, Splunk uses a random value to name the machine or device that generated the logs.
 - Update the value to “Windows_server_logs” and then select “Review”.
5. On the “Review” page, verify that you've chosen the correct settings.
 - Select “Submit” to proceed with uploading your data into Splunk.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.
7. Select “Start Searching.”
8.  **Important:** After the data populates on the search, select “All Time” for the time range.

Part 2: Analyze Windows Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created in Day 1 and analyze the results. To do so, complete the following steps:

Report Analysis for Severity

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different severities.
3. Select “Open in Search.”
4. Take note of the percentages of different severities.
5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the [Project 3 Review Questions](#) document:
 - Did you detect any suspicious changes in severity?

Note: You will use this same document for the remaining review questions.

Report Analysis for Failed Activities

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that you created to analyze the different activities.
3. Select “Open in Search.”
4. Take note of the failed activities percentage.
5. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
6. Select “Save.”
7. Review the updated results, and answer the following question in the review document:

- Did you detect any suspicious changes in failed activities?

Now, you will review the alerts that you created on Day 1 and analyze the results.

Alert Analysis for Failed Windows Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of failed activities.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
5. Review the updated results, and answer the following questions in the review document (*note that your alerts will not trigger; this is a theoretical exercise*):
 - Did you detect a suspicious volume of failed activity?
 - If so, what was the count of events in the hour(s) it occurred?
 - When did it occur?
 - Would your alert be triggered for this activity?
 - After reviewing, would you change your threshold from what you previously selected?

Alert Analysis for Successful Logins

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of successful logins.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.

5. Review the updated results, and answer the following questions in the review document:
 - Did you detect a suspicious volume of successful logins?
 - If so, what was the count of events in the hour(s) it occurred?
 - Who is the primary user logging in?
 - When did it occur?
 - Would your alert be triggered for this activity?
 - After reviewing, would you change your threshold from what you previously selected?

Alert Analysis for Deleted Accounts

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of deleted accounts.
3. Select “Open in Search.”
4. Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
5. Review the updated results, and answer the following question in the review document:
 - Did you detect a suspicious volume of deleted accounts?

Next, you will view your dashboard and analyze the results.

Dashboard Setup

1. Access the Windows Web Server Monitoring dashboard.
 - Select “Edit.”
2. For each panel that you created, access the panel and complete the following steps:

- Select “Edit Search.”
- Change the source from `windows_server_logs.csv` to `source="windows_server_attack_logs.csv"`.
- Select “Apply.”
- Save the dashboard.
- Change the time on the whole dashboard to “All Time.”

Dashboard Analysis for Time Chart of Signatures

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- What signatures stand out?
- What time did each signature’s suspicious activity begin and stop?
- What is the peak count of the different signatures?

Dashboard Analysis for Users

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Which users stand out?
- What time did each user's suspicious activity begin and stop?
- What is the peak count of the different users?

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Do the results match your findings from the time chart for signatures?

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Do the results match your findings from the time chart for users?

Dashboard Analysis for Users with Statistical Charts

Analyze your new dashboard results, and answer the following question in the review document:

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?


Checkpoint

Before continuing, make sure that you have completed the following critical tasks:

- ✓ Loaded Windows attack logs.
- ✓ Changed the source in the reports, alerts, and dashboards.
- ✓ Analyzed the attack data and answered the review questions.

Part 3: Load Apache Attack Logs

In this part, you will upload Apache attack logs into your Splunk environment. To do so, complete the following steps:

1. Return to the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
 - Click “Select File.”
 - Select the `apache_attack_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
 - Click the green “Next” button on the top right.
3. You will be brought to the “Set Source Type” page.
 - You don’t need to change any configurations on this page.
 - Select “Next” again.
4. You'll be brought to a page called “Input Settings.”
 - This page contains optional settings for how the data is input.
 - In the “Host” field value, Splunk uses a random value to name the machine or device that generated the logs.
 - Update the value to “Apache_logs” and then select “Review.”
5. At the “Review” page, verify that you've chosen the correct settings.
 - Select “Submit” to proceed with uploading your data into Splunk.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear.
7. Select “Start Searching.”
8.  **Important:** After the data populates on the search, select “All Time” for the time range.

Part 4: Analyze Apache Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created on Day 1 and analyze the results. To do so, complete the following steps:

Report Analysis for Methods

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP methods.
3. Select “Edit” > “Open in Search.”
4. Take note of the percent and count of the various methods.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
6. Select “Save.”
7. Review the updated results, and answer the following questions in the review document:
 - Did you detect any suspicious changes in HTTP methods? If so, which one?
 - What is that method used for?

Report Analysis for Referrer Domains

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different referrer domains.
3. Select “Edit” > “Open in Search.”
4. Take note of the different referrer domains.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
6. Select “Save.”

7. Review the updated results, and answer the following question in the review document:
 - Did you detect any suspicious changes in referrer domains?

Report Analysis for HTTP Response Codes

1. Access the “Reports” tab, and select “Yours” to view the reports that you created on Day 1.
2. Select the report that analyzes the different HTTP response codes.
3. Select “Edit” > “Open in Search.”
4. Take note of the different HTTP response codes.
5. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
6. Select “Save.”
7. Review the updated results and answer the following question in the review document:
 - Did you detect any suspicious changes in HTTP response codes?

Now, you will review the alerts that you created on Day 1 and analyze the results.

Alert Analysis for International Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of international activity.
3. Select “Open in Search.”
4. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
5. Review the updated results, and answer the following questions in the review document:

- Did you detect a suspicious volume of international activity?
- If so, what was the count of events in the hour(s) it occurred?
- Would your alert be triggered for this activity?
- After reviewing, would you change the threshold you previously selected?

Alert Analysis for HTTP POST Activity

1. Access the “Alerts” tab, and select “Yours” to view the alerts that you created on Day 1.
2. Select the alert for suspicious volume of HTTP POST activity.
3. Select “Open in Search.”
4. Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
5. Review the updated results, and answer the following questions in the review document:
 - Did you detect any suspicious volume of HTTP POST activity?
 - If so, what was the count of events in the hour(s) it occurred?
 - When did it occur?
 - After reviewing, would you change the threshold that you previously selected?

Now, you will set up a dashboard and analyze the results.

Dashboard Setup

1. Access the Apache Web Server Monitoring dashboard.
2. Select “Edit.”
3. For each panel that you created, access the panel and complete the following steps:

- Select “Edit Search.”
 - Change the source from `source=apache_logs.txt` to `source="apache_attack_logs.txt"`.
 - Select “Apply.”
4. Save the whole dashboard.
 5. Change the time on the whole dashboard to “All Time.”

Dashboard Analysis for Time Chart of HTTP Methods

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Which method seems to be used in the attack?
- At what times did the attack start and stop?
- What is the peak count of the top method during the attack?

Dashboard Analysis for Cluster Map

Analyze your new cluster map results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- Which new location (city, country) on the map has a high volume of activity?
 - **Hint:** Zoom in on the map.
- What is the count of that city?

Dashboard Analysis for URI Data

Analyze your dashboard panel of the URI data, and answer the following questions in the review document:

- Does anything stand out as suspicious?
- What URI is hit the most?
- Based on the URI being accessed, what could the attacker potentially be doing?

Part 5: Create Project Presentations

In this part, you will begin to create a presentation to showcase the work you completed during your project.

Use the following framework to design your team's presentation: [Project 3 Presentation Framework](#).

1. First, make a copy of this presentation.
2. Complete all of the required items in square brackets.
 - Use your review guide to assist you.
3. Feel free to be creative in your project presentations.
 - Add any additional slides that you would like.
 - Add any additional visualizations, images, videos, etc. that you would like.
4. Prioritize spending more of your presentation time on your unique "Add-On" application.
5. Feel free to split up the work on this presentation, but remember that every student must submit their own complete presentation (even if it is a copy of your other team members').

Day 2 Milestones

In today's class, you completed the following steps:

1. **Loaded Windows attack logs.**

- 2. Analyzed Windows attack logs.**
- 3. Loaded Apache attack logs.**
- 4. Analyzed Apache attack logs.**
- 5. Began creating project presentations.**

In the next class, you will present your monitoring environment and findings to the class!