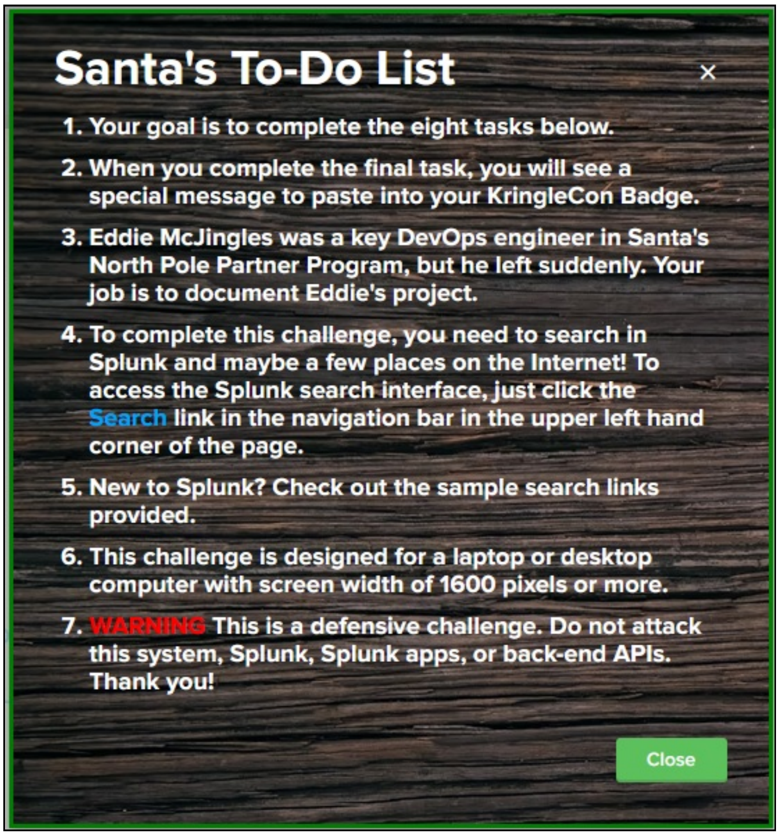
KringleCon 4: Calling Birds!

9) Splunk!

1. Click `Map` (Destinations) icon and then click `Great Room`

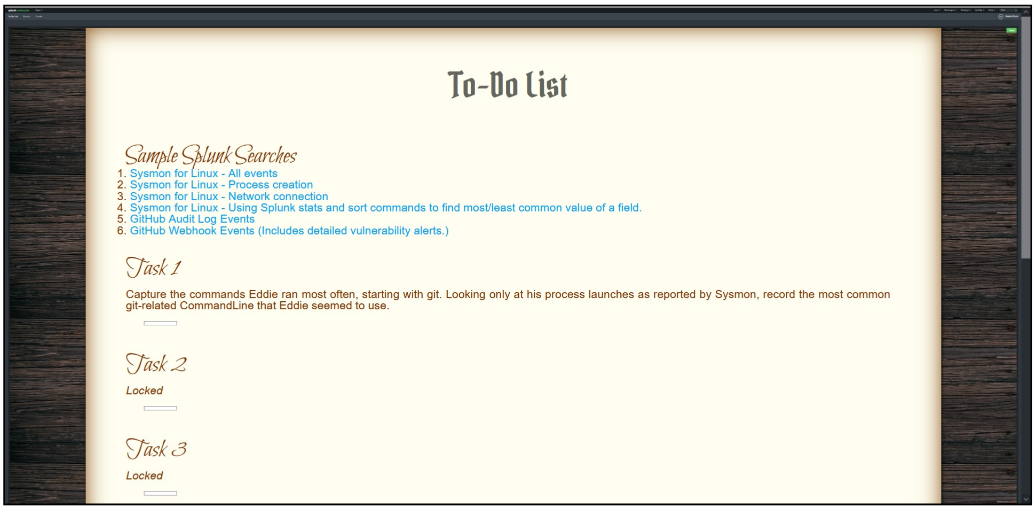
2. Click `splunk` Cranberry Pi terminal



Santa's To-Do List

1. Your goal is to complete the eight tasks below.
2. When you complete the final task, you will see a special message to paste into your KringleCon Badge.
3. Eddie McJingles was a key DevOps engineer in Santa's North Pole Partner Program, but he left suddenly. Your job is to document Eddie's project.
4. To complete this challenge, you need to search in Splunk and maybe a few places on the Internet! To access the Splunk search interface, just click the Search link in the navigation bar in the upper left hand corner of the page.
5. New to Splunk? Check out the sample search links provided.
6. This challenge is designed for a laptop or desktop computer with screen width of 1600 pixels or more.
7. WARNING This is a defensive challenge. Do not attack this system, Splunk, Splunk apps, or back-end APIs. Thank you!

3. Click the `Close` button



To-Do List

Sample Splunk Searches

1. Sysmon for Linux - All events
2. Sysmon for Linux - Process creation
3. Sysmon for Linux - Network connection
4. Sysmon for Linux - Using Splunk stats and sort commands to find most/least common value of a field.
5. GitHub Audit Log Events
6. GitHub Webhook Events (Includes detailed vulnerability alerts.)

Task 1

Capture the commands Eddie ran most often, starting with git. Looking only at his process launches as reported by Sysmon, record the most common git-related CommandLine that Eddie seemed to use.

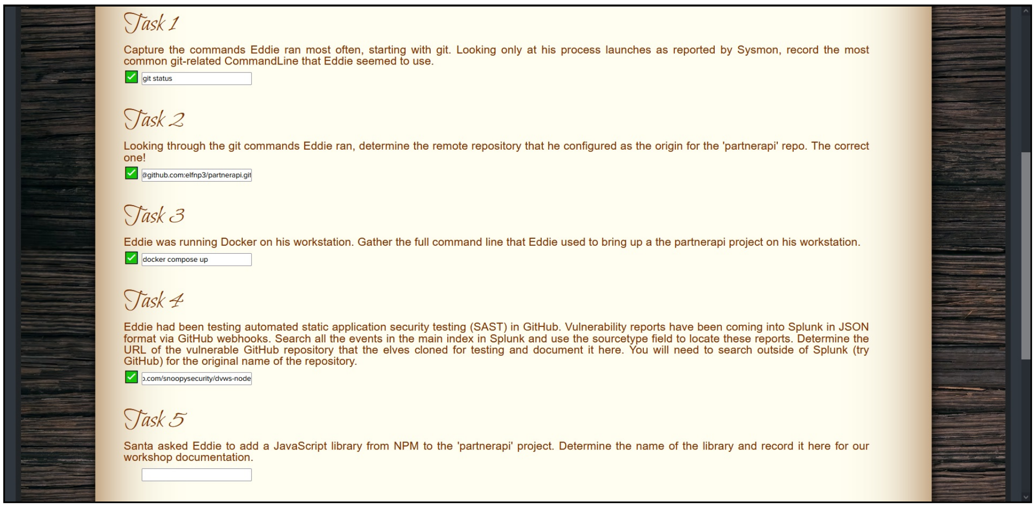
Task 2

Locked

Task 3

Locked

4. Complete the Tasks



Task 1

Capture the commands Eddie ran most often, starting with git. Looking only at his process launches as reported by Sysmon, record the most common git-related CommandLine that Eddie seemed to use.

☑ git status

Task 2

Looking through the git commands Eddie ran, determine the remote repository that he configured as the origin for the 'partnerapi' repo. The correct one!

☑ @github.com:elfnp3/partnerapi.git

Task 3

Eddie was running Docker on his workstation. Gather the full command line that Eddie used to bring up a the partnerapi project on his workstation.

☑ docker compose up

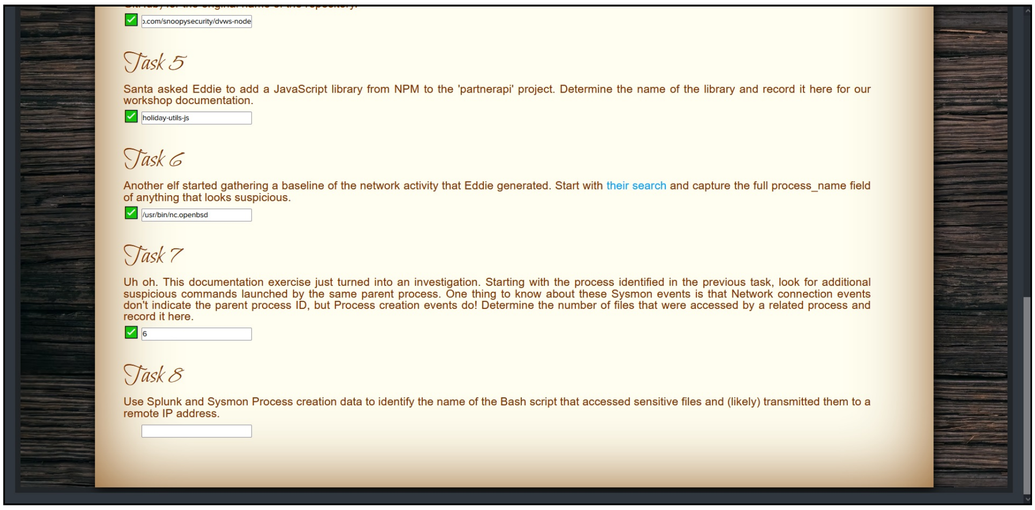
Task 4

Eddie had been testing automated static application security testing (SAST) in GitHub. Vulnerability reports have been coming into Splunk in JSON format via GitHub webhooks. Search all the events in the main index in Splunk and use the sourcetype field to locate these reports. Determine the URL of the vulnerable GitHub repository that the elves cloned for testing and document it here. You will need to search outside of Splunk (try GitHub) for the original name of the repository.

☑ ›.com/snoopysecurity/dvws-node

Task 5

Santa asked Eddie to add a JavaScript library from NPM to the 'partnerapi' project. Determine the name of the library and record it here for our workshop documentation.



GitHub) for the original name of the repository.

☑ ›.com/snoopysecurity/dvws-node

Task 5

Santa asked Eddie to add a JavaScript library from NPM to the 'partnerapi' project. Determine the name of the library and record it here for our workshop documentation.

☑ holiday-utils-js

Task 6

Another elf started gathering a baseline of the network activity that Eddie generated. Start with their search and capture the full process_name field of anything that looks suspicious.

☑ /usr/bin/nc.openbsd

Task 7

Uh oh. This documentation exercise just turned into an investigation. Starting with the process identified in the previous task, look for additional suspicious commands launched by the same parent process. One thing to know about these Sysmon events is that Network connection events don't indicate the parent process ID, but Process creation events do! Determine the number of files that were accessed by a related process and record it here.

☑ 6

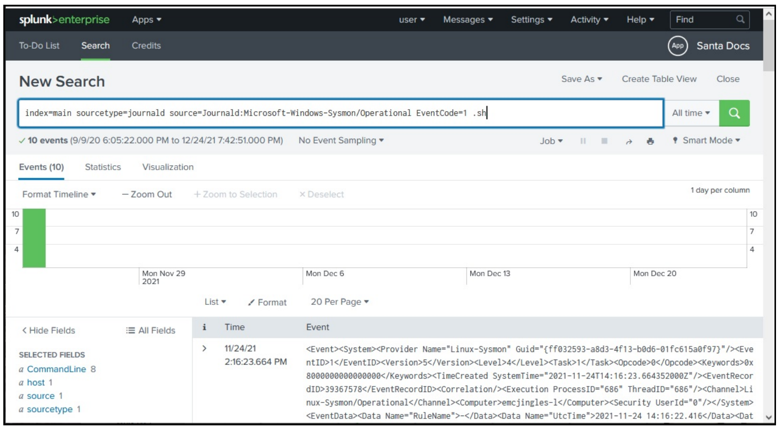
Task 8

Use Splunk and Sysmon Process creation data to identify the name of the Bash script that accessed sensitive files and (likely) transmitted them to a remote IP address.

5. Click the `Third` tab

6. Modify the Search to `index=main sourcetype=journald source=Journald:Microsoft-Windows-Sysmon/Operational EventCode=1 .sh`

7. Click the `Search` button



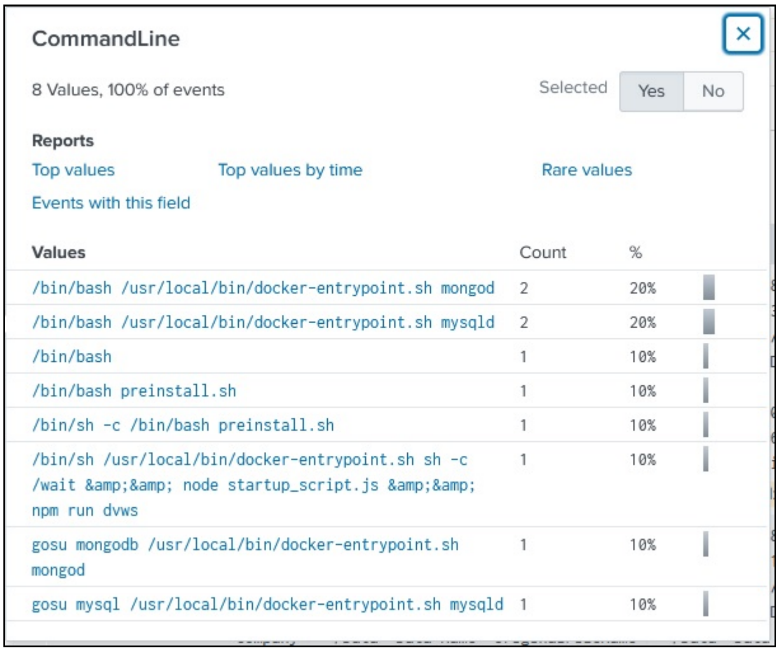
```
index=main sourcetype=journald source=Journald:Microsoft-Windows-Sysmon/Operational EventCode=1 .sh
```

✓ 10 events (9/9/20 6:05:22.000 PM to 12/24/21 7:42:51.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a CommandLine 8
- a host 1
- a source 1
- a sourcetype 1

i	Time	Event
›	11/24/21 2:16:23.664 PM	`<Event><System><Provider Name="Linux-Sysmon" Guid="{ff032593-a8d3-4f13-b0d6-01fc615a0f97}"/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2021-11-24T14:16:23.664352000Z"/><EventRecordID>39367578</EventRecordID><Correlation/><Execution ProcessID="686" ThreadID="686"/><Channel>Linux-Sysmon/Operational</Channel><Computer>emcjingles-l</Computer><Security UserId="0"/></System><EventData><Data Name="RuleName">-</Data><Data Name="UtcTime">2021-11-24 14:16:22.416</Data><Dat`

8. Click `CommandLine`



CommandLine

8 Values, 100% of events

Reports

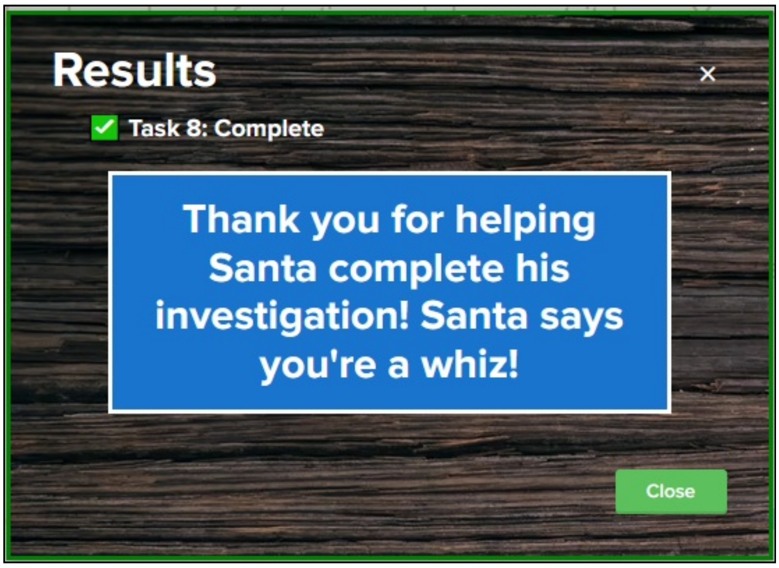
Top values Top values by time Rare values

Events with this field

Values	Count	%
/bin/bash /usr/local/bin/docker-entrypoint.sh mongod	2	20%
/bin/bash /usr/local/bin/docker-entrypoint.sh mysqld	2	20%
/bin/bash	1	10%
/bin/bash preinstall.sh	1	10%
/bin/sh -c /bin/bash preinstall.sh	1	10%
/bin/sh /usr/local/bin/docker-entrypoint.sh sh -c /wait &amp;&amp; node startup_script.js &amp;&amp; npm run dvws	1	10%
gosu mongodb /usr/local/bin/docker-entrypoint.sh mongod	1	10%
gosu mysql /usr/local/bin/docker-entrypoint.sh mysqld	1	10%

9. Close the `Third` tab

10. Type `preinstall.sh`



Results

✓ Task 8: Complete

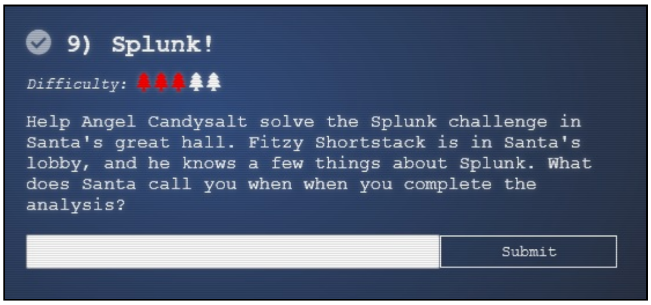
Thank you for helping Santa complete his investigation! Santa says you're a whiz!

11. Click the `Close` button

12. Close the `Second` tab

13. Click `Tick` (Objectives) icon

14. Click `9) Splunk!`



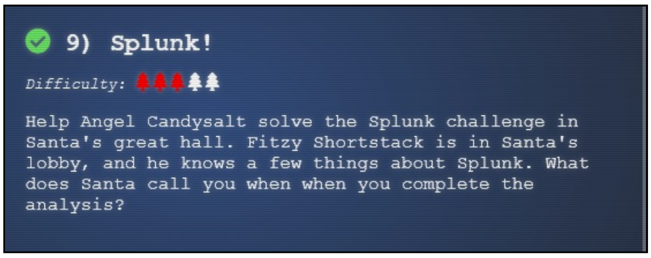
9) Splunk!

Difficulty: 🎄🎄🎄🎄🎄

Help Angel Candysalt solve the Splunk challenge in Santa's great hall. Fitzy Shortstack is in Santa's lobby, and he knows a few things about Splunk. What does Santa call you when when you complete the analysis?

15. Type `whiz`

16. Click the `Submit` button



9) Splunk!

Difficulty: 🎄🎄🎄🎄🎄

Help Angel Candysalt solve the Splunk challenge in Santa's great hall. Fitzy Shortstack is in Santa's lobby, and he knows a few things about Splunk. What does Santa call you when when you complete the analysis?