CYB102 Project 5

(🔗 Instructions Page)

👤 Student Name: [ ]
✉️ Student Email: [ ]

Reflection (Required)

> 🤔 **Reflection Question #1:** If I had to **explain "what is SIEM" in 3 emojis,** they would be…
> (Feel free to put other comments about your experience in this unit here, too!)
>
> 🔍📁🤔
> This is one of my favorite projects we have worked on thus far.

> 🧠**Reflection Question #2:** What field do you think is most important for logs to have?
>
> I would say having some kind of time field is very important. Knowing the time that events occurred is very useful in putting together the sequence of events that occurred when analyzing attacks. For instance, in Splunk, we were able to see when users logged in and when files were uploaded which allowed us to make a timeline of what happened at PathCode Inc. Without a time field, it is difficult to determine if an event occurred today, yesterday, or the week before.

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!
>
> Shoutout to myself for starting early on this project.

CTF Challenges (Required)

Use the answer boxes below to document any CTF challenges you completed.

- For each challenge, document both:
    1. The challenge answer
    2. The search command used to find the answer
- If you don't complete a particular challenge, leave it blank.

Part 1 - Searching the Netflix Data (1pt each)

index=main source=Netflix

👥 **Challenge 1:** How many TV shows on Netflix are in the Docuseries genre?

Solution:

1. **170**
2. index=main host=Netflix type="TV Show" listed_in=”Docuseries”

👥 **Challenge 2:** How many movies on Netflix have a rating of TV-PG?

Solution:

1. **1080**
2. index=main host=Netflix type=”Movie” rating=”TV-PG”

👥 **Challenge 3:** How many movies on Netflix were released in the year 2020?

Solution:

1. **1034**
2. index=main host=Netflix type=”Movie” release_year=”2020”

👥 **Challenge 4:** What is the longest duration by season on Netflix, and what is its TV rating?

Solution:

1. **17 Seasons (Grey’s Anatomy), TV-14**
2. index=main host=Netflix | eval season_count = tonumber(replace(duration, " Seasons", "")) | sort - season_count | table title, duration, season_count, rating

👥 **Challenge 5:** How many movies on Netflix are listed as action and are rated PG-13?

Solution:

1. **296**
2. index=main host=Netflix type="Movie" Action rating="PG-13"

👥 **Challenge 6:** How many movies and TV shows on Netflix have their country of origin as Turkey?

Solution:

1. **210**
2. index=main host=Netflix country=”Turkey”

👥 **Challenge 7:** Which release year had the most movies rated G? (Not TV-G)

Solution:

1. **2009**
2. index=main host=Netflix type=”Movie” rating=”G” | stats count by release_year | sort - count

👥 **Challenge 8:** What two TV-Y7 rated shows were released in 2019 and were added to Netflix on November 22, 2019?

Solution:

1. **Trolls: The Beat Goes on!, The Dragon Prince**
2. index=main host=Netflix rating =”TV-Y7” release_year=”2019” date_added=”November 22, 2019” | dedup title | table title

👥 **Challenge 9:** Which year had the most movies from the United States?

Solution:

1. **2017**
2. index=main host=Netflix type=”Movie” country=”United States” | stats count by release_year | sort - count

👥 **Challenge 10:** What is the oldest TV show by Release Year on Netflix?

Solution:

1. **Pioneers: First Women Filmmakers***
2. index=main host=Netflix type=”TV Show” | sort release_year | dedup title | table title, release_year

Part 2 - Investigating the Malware (2pts each)

For Part 2 we are investigating an attacker who got into our systems that happened at PathCode Inc.
For these logs use index=pathcode

👥 **Challenge 11:** What was the IP address that uploaded the malware (MD5 hash: 3AADBF7E527FC1A050E1C97FEA1CBA4D)

Solution:

1. **192.168.1.10**
2. index=pathcode “File Hash”=”3AADBF7E527FC1A050E1C97FEA1CBA4D” | table host, IP

👥 **Challenge 12:** What usernames did that IP address try to login to the system as? Which one did they upload a file as?

Solution:

1. **ABurke <- Uploaded file as**
   Pi
   Admin
2. index=pathcode IP="192.168.1.10" ("Login Failed" OR "Login Attempt" OR "File Uploaded" OR "File Upload") | table Username, Filename, Event

👥 **Challenge 13:** What was the User Agent String of the attacker when they successfully uploaded a file?

Solution:

1. **Opera/75.0.3969.218**
2. index=pathcode IP="192.168.1.10" Event="File Uploaded"

👥 **Challenge 14:** Did any other users also upload a file around that time? If so, who and what was their IP address?

Solution:

1. **Jmann, 192.168.1.7**
2. index=pathcode Event=”File Upload” | table _time, Username, IP

> 👥 **Challenge 15:** Looking at the uploaded hashes, what were the files called that the two users uploaded? Which one seems like it was malicious?
>
> **Solution:**
>
> 1. **proposal.pdf,**
>   **EvilScript.exe <- seems malicious**
> 2. index=pathcode Event="File Uploaded" ("192.168.1.10" OR "192.168.1.7") | table _time, Filename, "File Hash"

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Reflection

- ☑ ~~Reflection Question #1 answered above~~
- ☑ ~~Reflection Question #2 answered above~~

CTF Challenges (10pts needed for full credit, 17pts needed for extra credit)

Part 1 - 1pt each

- ☑ ~~Challenge #1: How many TV shows on Netflix are in the Docuseries genre?~~
- ☑ ~~Challenge #2: How many movies on Netflix have a rating of TV-PG?~~
- ☑ ~~Challenge #3: How many movies on Netflix were released in the year 2020?~~
- ☑ ~~Challenge #4: What is the longest duration by season on Netflix, and what is its TV rating?~~
- ☑ ~~Challenge #5: How many movies on Netflix are listed as action and are rated PG-13?~~
- ☑ ~~Challenge #6: How many movies and TV shows on Netflix have their country of origin as Turkey?~~
- ☑ ~~Challenge #7: Which release year had the most movies rated G? (Not TV-G)~~
- ☑ ~~Challenge #8: What two TV-Y7 rated shows were released in 2019 and were added to Netflix on November 22, 2019?~~
- ☑ ~~Challenge #9: Which year had the most movies from the United States?~~
- ☑ ~~Challenge #10: What is the oldest TV show by Release Year on Netflix?~~

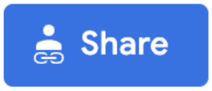
Part 2 - 2pts each

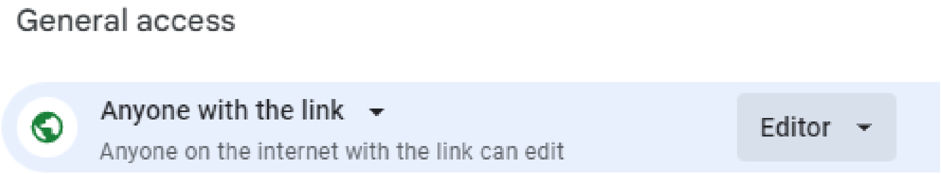
- ☑ ~~Challenge #11: What was the IP address that uploaded the malware (MD5 hash: 3AADBF7E527FC1A050E1C97FEA1CBA4D)~~
- ☑ ~~Challenge #12: What usernames did that IP address try to login to the system as? Which one did they upload a file as?~~
- ☑ ~~Challenge #13: What was the User Agent String of the attacker when they successfully uploaded a file?~~
- ☑ ~~Challenge #14: Did any other users also upload a file around that time? If so, who and what was their IP address?~~
- ☑ ~~Challenge #15: Looking at the uploaded hashes, what were the files called that the two users uploaded? Which one seems like it was malicious?~~

💡***Tip: You can see specific grading information, including points breakdown, by going to 🔗 the grading page on the course portal.***

Submit your work!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.



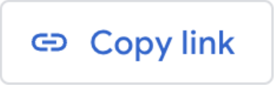

General access

Anyone with the link

Anyone on the internet with the link can edit

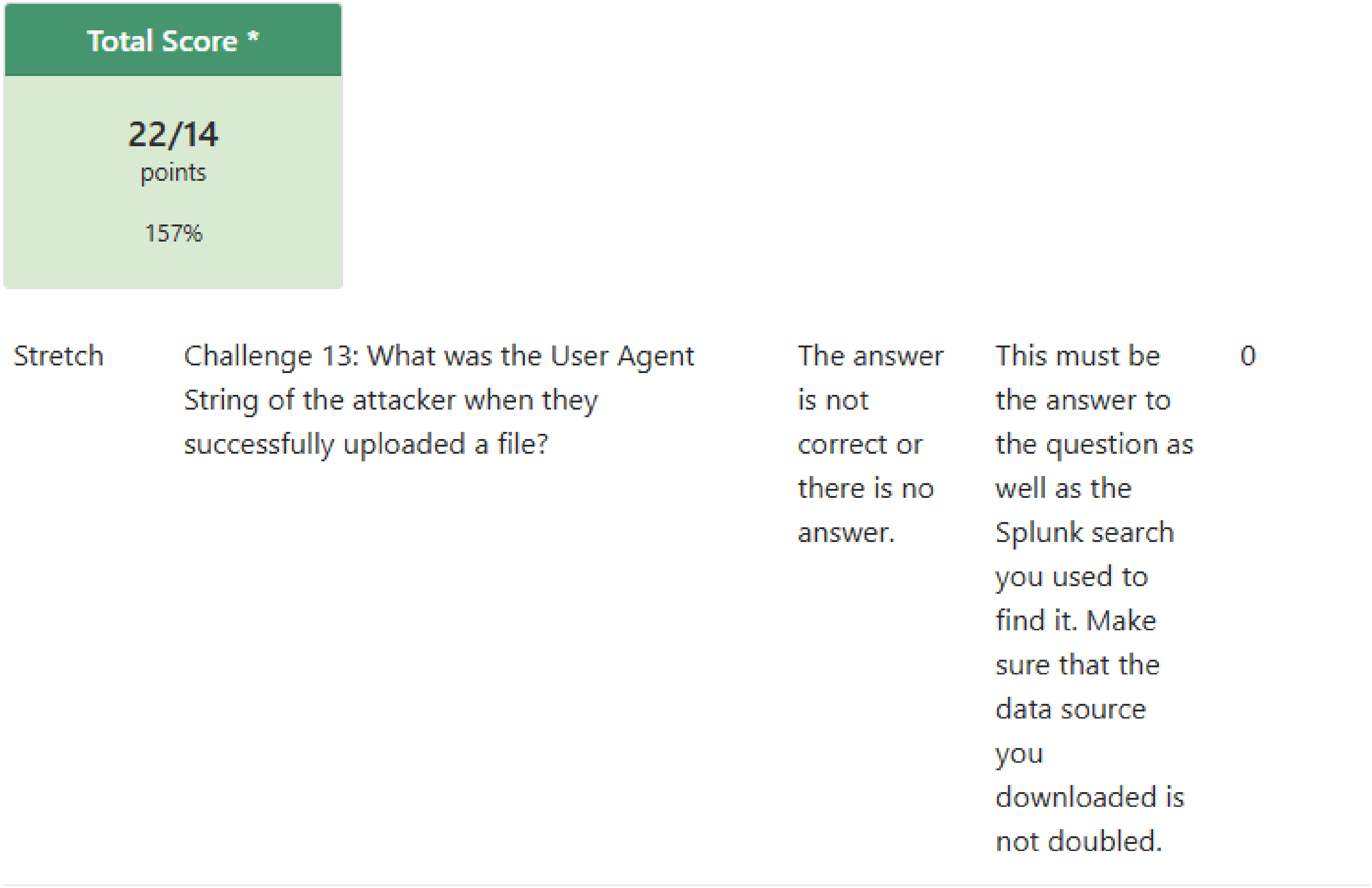
Editor

Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.

Grading



Total Score *

22/14

points

157%

Stretch	Challenge 13: What was the User Agent String of the attacker when they successfully uploaded a file?	The answer is not correct or there is no answer.	This must be the answer to the question as well as the Splunk search you used to find it. Make sure that the data source you downloaded is not doubled.	0