CYB102 Project 5

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicongx.wx@gmail.com

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!)
>
> 🔍🛡️📊

> 🧠**Reflection Question #2:** What field do you think is most important for logs to have?
>
> The IP address

> 📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

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. 790
2. index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type="TV Show" listed_in="*Docuseries*"

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

Solution:

1. 1,080
2. index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type=Movie rating="TV-PG"

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

Solution:

1. 1,034
2. index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" 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, TV-14
2. index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type="TV Show" duration="17 Seasons"

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

Solution:

1. 296
2. index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type="Movie" rating="PG-13" listed_in="*Action & Adventure*"

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

Solution:

1. 226
2.
   ```
   index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" country="*Turkey*"
   ```

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

Solution:

1. 2009
2.
   ```
   index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" 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 source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type="TV Show" release_year="2019" rating="TV-Y7" date_added="November 22, 2019"
   ```

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

Solution:

1. 2017
2.
   ```
   index=main source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" 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 source="/home/codepath/Files/Splunk-5-6-7/netflix_titles.csv" type="TV Show" release_year="1925"
   ```

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

> 👥 **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, Admin, Pi
>   File uploaded by ABurke
> 2. index="pathcode" IP="192.168.1.10" Event="Login Attempt"
>   index="pathcode" IP="192.168.1.10" Event="File Upload"

> 👥 **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. 192.168.1.7 — Firefox/89.0 — Jmann

> 2. index="pathcode" Event="File Upload"

> 👥 **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. EvilScript.exe — proposal.pdf
> 2. index="pathcode" Event="File Uploaded" IP="192.168.1.10"
>   index="pathcode" Event="File Uploaded" IP="192.168.1.7"

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?~~