


Project 5

Gerrell Bones
02 NOV 2023
CNT 4403
Project 5

Part 1 - Searching the Netflix Data (10pts each)

index=main source=Netflix

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

Solution:

1. 85 Total:
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. 540 total
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. 46 total
2. **index="main" host="Netflix" type="Movie" rating="TV-PG"
release_year=2020**

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

Solution:

1. 107 Minutes and TV-PG
2. **index="main" host="Netflix" type="Movie" rating="TV-PG" release_year=2020 duration="107 min"**

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

Solution:

1. 23 total
2. **index="main" host="Netflix" 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. 105 Total
- 2.

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

Solution:

1. 2009
- 2.

👤 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!
2. The Dragon Prince

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

Solution:

1. 2014
- 2.

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

Solution:

1. Pioneers: First Women Filmmakers
- 2.

Part 2 – Investigating the Malware (20pts 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: 3AADB7E527FC1A050E1C97FEA1CBA4D)

Solution:


1. 192.168.1.10
- 2.

👤 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. Admin / PI / ABurke

2. Aburke

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


Solution:

1. Opera/75.0.3969
- 2.

 **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
- 2.

 **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. EvilScript.exe