Capture the Flag (CTF) Write-Up - Alvin Sarkadi

Section I: The Solves

10 CTF challenges

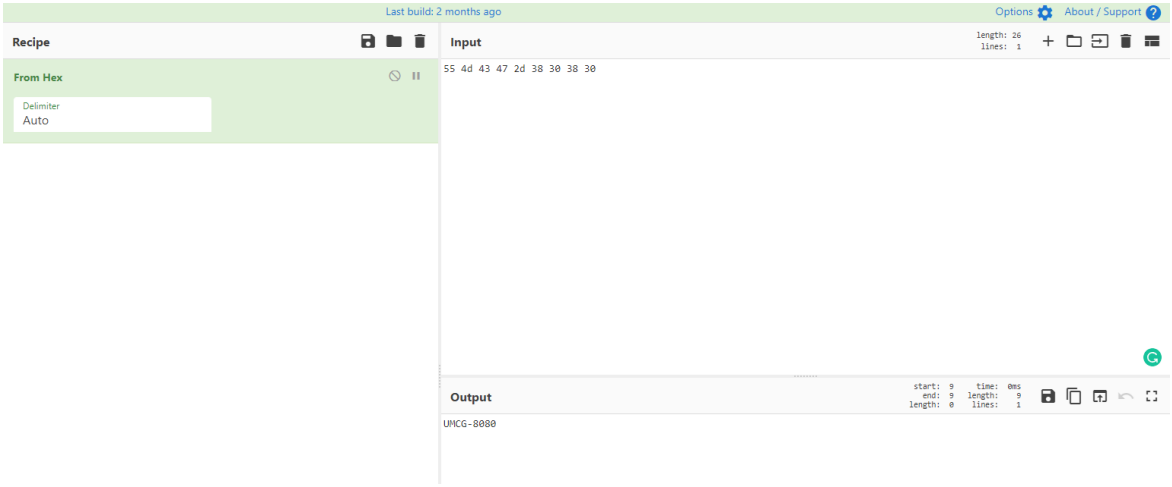
- *Category 1 Challenge 3*

Converting hexicadecimal to String (ASCII)

The following Hex was: 55 4d 43 47 2d 38 30 38 30

I used an open source tool called Cyberchef to convert the Hex input into the following string:

UMGC-8080



2.

- *Category 7 Challenge 4*

How many games did the Brooklyn Superbas lose in 1904

According to my search engine (firefox), the Brookyln Superbas lost 97 games.

https://www.baseball-almanac.com/teamstats/roster.php?y=1904&t=BR6#:~:text=The%201904%20Brooklyn%20Superbas%20played,and%20finished%20in%20sixth%20position.

- *Category 8 Challenge 1*

Given the hash below, find the password for the user listed.

bart:"":"":A988BBFD3CFDE311AAD3B435B51404EE:9CE736F7B01B851A7BBB9DA1B67E6C98

For this challenge, I again used cyberchef. Cyberchef includes a hashing tool. When inputting the hash and generating an output using MD2 and MD5, I was able to generate 2 passwords. The following passwords appeared:

MD5 Password Output: d12be87b8c75716e119ab5597dc0fd2a

MD2 Password Output: dfc30802d50348b220b90b7f72e56b90

.Category 4 Challenge 1:

Use the IIS log to determine what version of curl was used by the web client.

7.19.7

When opening the file in notepad++ and searching for 'curl', I was able to see the curl version the user was running. (Crtl+F, find 'curl')

.Category 4 Challenge 3:

Use the IIS log to determine the version of Wget was used by a client.

Wget version: 1.12+

Category 4 Challenge 4:

How many times does Mozilla appear in the file?

12155 matches found. Using the find tool in notepad++, I was able to count how many times the log file includes the word 'Mozilla'

Category 4 Challenge 6:

How many times does 331 appear in the file?

180855 matches in entire file.

Category 7 - Challenge 9:

What was the Apache web server version for pgcps.org in 2011?

August 2011, the version for Apache was 2.2.20

Category 4 Challenge 5:

Use the IIS log to determine how many times the IP address 192.168.1.50 appears in the file.

12088 matches in entire file

Category 4 Challenge 8:

Use the IIS log to determine what country is the attack on this server coming from.

The file included no details regarding the attack origin (besides the IP.)

When doing a simple trace of the IP on a search engine, the attacker is based in Beijing, China

IP: 211.100.100.97

Category 4 Challenge 10:

Use the SMTP log to determine what time the hacker logs in successfully

Viewing the log file, I believe the attacker gained entry at: 23:57:54

Category 8 Challenge 2:

Given the hash below, find the password for the user listed.

snowball:"":"":D8C770C7E94592D9AAD3B435B51404EE:EEC1E8A883208C9A53FD91821F0EAB68

Cyberchef output for hashing:

MD2: 2be7ac42f7c38e77b4473a6b149e7762

MD4: 59f2f1acd6adb6948eff7bda24e77381

MD5: 6b6eeac23c9627657bb357810b141eb4

MD6: 6afa12b77637c4a7b82069f7a1ec0a3648618cf0e978c5ce6f66c7547926a0dd

SHA0: 1dbfa38e907027df6226758a4bf5465ab49f39e9

SHA1: d065482a1fbe87215135b2d50266960a39958d15

SHA2 224: 14d5794e99091f447882c0445d68d74841c71a711ecff97dcc2091aa

SHA2 256: 18decae0b6a955c47b8f0b8d7dade9a52df6763a7772e514d5ff5c20c67735d8

Section II: Strategies Employed

Explain how you approached two of the 10 CTF challenges you attempted and solved. For example, what techniques, tools, websites, or other resources did you use?

I really enjoyed the log analysis questions that I solved. Specifically the one where I had to find the attackers location. This was particularly intresting because there was no information about the attacker besides the IP. Even though I skimmed through the whole log, I realized the only information about the attacker is within the IP. So I decided to do a simple IP trace on a search engine, which led me to believe that the attackers origin is Beijing, China.

Another challenge I enjoyed doing was Category 1, Challenge 3. With this challenge I didn't know how Cyberchef and other cracking tools can be so useful and helpful. After getting familiar with cyberchef I noticed that the tool also offers hashing, which is what I used to crack the hashes for Category 8.

Section III: Lessons Learned

- What are your strengths/How would your skills benefit a CTF team?
- **I believe I am very detail oriented, and patient. I can sit through a log file for hours until I find what I need to move forward. I believe in a group scenario this would be beneficial because I can also be of great assistance if a team member needs help.**
- Which challenge banks did you find easy?
- **Log Analysis, Open Source intellegence, File Anaylsis**
- What areas do you need more practice in?
- **Network capturing, throughout my courses (including networking) I struggled with getting familiar with Wireshark. I find it very difficult since I do not like the UI, and I still struggle to understand some of the information being gathered during a capture.**
- Which challenge banks did you struggle with or avoid?

Virtual Machines, this is a category I really wanted to do, but ever since I reset my PC and installed Windows 11, all of my virtual machines via Oracle are not booting. Even the one provided by the professor. I believe its a personal BIOS issue I need to resolve.

- Were there challenges you attempted but did not complete or challenges that you did not attempt?
- **Category 4, Challenge 10 I was unable to identify the specific time the intruder got access when analyzing the log file provided. Although I provided an answer, I am unsure whether this is the correct time the intruder gained access.**
- How can you improve your skills in that area (strategies, tools, websites, etc.)?

The textbook and labs have been helpful. However, If I am unfamiliar with a topic, I use youtube to gain a initial understanding, and continue to watch videos and read articles on the topic to improve my knowledge.