Michael Lambinicio

CMIT321

April 5, 2022

Capture the Flag (CTF) Write-Up

Section I: The Solves

List the 10 CTF challenges you attempted.

1. Category 1: Challenge 2: Convert this to a dotted decimal notation IPv4 address
2. Category 1: Challenge 3: Convert the string below from hex to ASCII
3. Category 6: Challenge 1: In this capture file, what is the IP address of the SSH server
4. Category 6: Challenge 2: In this capture file, what is the FTP password with UMGC in it
5. Category 6: Challenge 4: In this capture file, find the admin's password
6. Category 7: Challenge 2: On May 26, 2002, UMGC held a graduation ceremony in Heidelberg and which other city
7. Category 7: Challenge 4: How many games did the Broooklyn Superbas lose in 1904
8. Category 7: Challenge 5: How many games did the Boston Bees win in 1936
9. Category 7: Challenge 7: Most likely, which National Football League team is Jesse Varsalone's favorite? Jesse is a professor at the University of Maryland Global Campus
10. Category 7: Challenge 8: What is the full name of the subdomain under umgc.edu that starts with an 'g'?
11. Category 2: Challenge 1: Identify the exact file name and extension if applicable

Section II: Strategies Employed

Would like to note that other than the challenges in Category 6, the remaining challenges (7) were utilizing research online.

1. For this challenge, I did a quick reference for definition of the numbers and understood that it was a binary system. I then looked for an online binary to ip converter and was able to produce the answer of **192.168.20.254**. The link used: https://www.browserling.com/tools/bin-to-ip
2. I did a search for hex to ASCII converter and copy/pasted the string in to get the result of: **UMCG-8080**. The link found was: https://www.rapidtables.com/convert/number/hex-to-ascii.html

3. For all of the challenges in category 6, I had to look up what program would .pcap work with to view the capture file. I was fortunate and lucky enough to have a previous program (Wireshark) installed from a previous course I took that allowed me to attempt this challenge. I opened up the capture files and to fin the answers to each of the questions, I could do a find for key words to simplify the search. I also had to understand that within the capture, that finding IP and passwords follow certain protocols (i.e utilizing FTP and HTTP as points to know how users log in). SMTP which uses mail, does not provide the same user and pass as admin user/pass). For Challenge 1, the answer is: **192.168.1.200**. Challenge 2, the answer was: **UMGC-234562**. Challenge 4 gave an answer of: **UMGC-5545512**.
4. For all of the challenges in category 7, I just researched all answers through Google. On question 2, the answer is: **Seoul**. When I first did my research using UMGC as the name, there was no accurate answer. I had to revert back to the old name, University Maryland University College. Link: (https://www.washingtonpost.com/archive/local/2002/05/18/graduations-travel-the-time-zones/71b94d7e-5b38-46a6-8621-784971e291c0/) For challenge 4, it is **97**. Link https://www.baseball-reference.com/teams/BRO/1904.shtml.Challenge 5, it is: **71**. Link:https://www.baseball-almanac.com/teamstats/roster.php?y=1936&t=BS6 Challenge 7: **ravens**. When I typed his name and NFL team, the first result was a comment he made from ESPN. Link: https://m.facebook.com/NFLonESPN/photos/a.104466009651775/2706453546119662/?comment_id=2706468262784857. As for challenge 8: **gear.umgc.edu**. This challenge I had to utilize a sub-domain analyzer to get a full list of subdomains. Link: https://scantrics.io/subdomain-scanner/
5. The one challenge that I saw but did not attempt was category 2, challenge 1. I realized that I did not even know where to begin…

Section III: Lessons Learned

- Being able to research online and find available online tools (if I understand the assignment) would be a strength I believe I have. I am a little savvy when using certain applications. I can follow directions when learning programs, but I mainly remember through repetition. All of the research (open source intelligence) challenges seemed to be easy; with the exception of find certain applications that are obsolete, or I just could not find it doing a regular search and meta search. I think that I am very novice at this pen-testing side, so all applications used I would need a good amount of time using it and being hands on it frequently. As for the struggles of the remaining categories, I believe I was struggling through it all. It was a little helpful to be informed that taking what are doing in the labs and applying to this project is where you can find some of the solutions. I think I would need a "tutor" on how to run through these challenges; I really doesn't feel good to be the weakest link…