|  |  |
| --- | --- |
| Capture the Flag (CTF) Write-Up Misty Keefe | Corporate Logo |

**Section I: The Solves**

1. *Category 1 Challenge 2*
   * *Answer: 192.168.20.254*
2. *Category 2 Challenge 2*
   * *Answer: elf.exe*
3. *Category 3 Challenge 2*
   * *Answer: 07/08/2013*
4. *Category 4 Challenge 2*
   * *Answer: 2.1.6*
5. *Category 5 Challenge 2*
   * *Answer:* *1.1.1.1:1234*
6. *Category 6 Challenge 2*
   * *Answer: UMGC-234562*
7. *Category 7 Challenge 2*
   * *Answer: Seoul*
8. *Category 8 Challenge 2*
   * *Answer: my cat*
9. *Category 9 Challenge 2*
   * *Answer: version7*
10. *Category 10 Challenge 2*
    * *Answer:* CTF-999115

**Section II: Strategies Employed**

This is my first time attempting CTF challenges. I reviewed the provided class material of the book, labs, and CTF strategies to be able to conquer most of these challenges. One of easiest challenge was the Category 1 Challenge 2, to convert decimal notation to IPv4 addrese. I have experience with subnetting and could have done this on paper using my brain, but I decided to use google for a faster, more reliable option. The website that I used to convert the decimal to IPv4 was called Browserling. It was super easy to use and produced the correct answer when I completed the quiz in classroom. One of the more difficult challenges was Category 6 Challenge 2, which was to determine the FTP password. In Wireshark, I imported the file then used the filter to enter in FTP. Wireshark filtered all the packets and only showed me packets that were using the FTP protocol which made it easier to find the password.

**Section III: Lessons Learned**

I am very new to CTF challenges and have a lot to work on. Participating in this CTF greatly assisted me in gaining practical experience with real-world problems. My strengths include the basic knowledge and familiarity of networking, cryptography, python, exploitation techniques. I just got my CompTIA Security Plus certification and know the theoretical knowledge of exploitation, securing networks, identifying vulnerabilities, implement security measures, and respond effectively to incidents. Although I don’t have much experience with prior ethical hacking problems, I will bring persistence, determination, analytical thinking, willingness to a CTF team. I will be able to communicate, collaborate, and cooperate within the team which will be paramount to the success of capturing our flags. The challenge banks that I found easy were 1,3,4,6,7,8. The areas that I need more practice in are fie analysis, malware analysis/reverse engineering, and scanning exploitation. The challenge banks that I tended to avoid or struggle with were the interactive file questions. As a MacBook user, I struggled and am still figuring out the VM setups and tried to use suggested software the best to my ability. The challenges that I attempted but did not complete were 5,9,10. I can improve my skills by familiarizing myself with the tools to gain confidence in the strategies for scanning exploitation.

Although this was my first CTF, it won’t be my last! I already signed up for hack the box, try hack me, and looked at over the wire. I had fun using problem-solving skills and analytical thinking to accomplish an objective. I’m especially excited for the group CTF happening next in this class!

**References**

**Browserling Inc. “Binary to IP Converter - Convert Bin to IP - Online.” Browserling, 2023,** [**https://www.browserling.com/tools/bin-to-ip. Accessed 3 July 2023**](https://www.browserling.com/tools/bin-to-ip.%20Accessed%203%20July%202023)**.**

*CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.*, 27 May 2019, https://crackstation.net/. Accessed 4 July 2023.

Virus Total. “Virus Total.” *VirusTotal - Home*, https://www.virustotal.com/gui/home/upload. Accessed 4 July 2023.

“MiTeC Homepage.” *MiTeC Homepage*, https://www.mitec.cz/wrr.html. Accessed 4 July 2023.

*Wireshark · Go Deep*, https://www.wireshark.org/. Accessed 4 July 2023.