

Capture the Flag (CTF) Write-Up

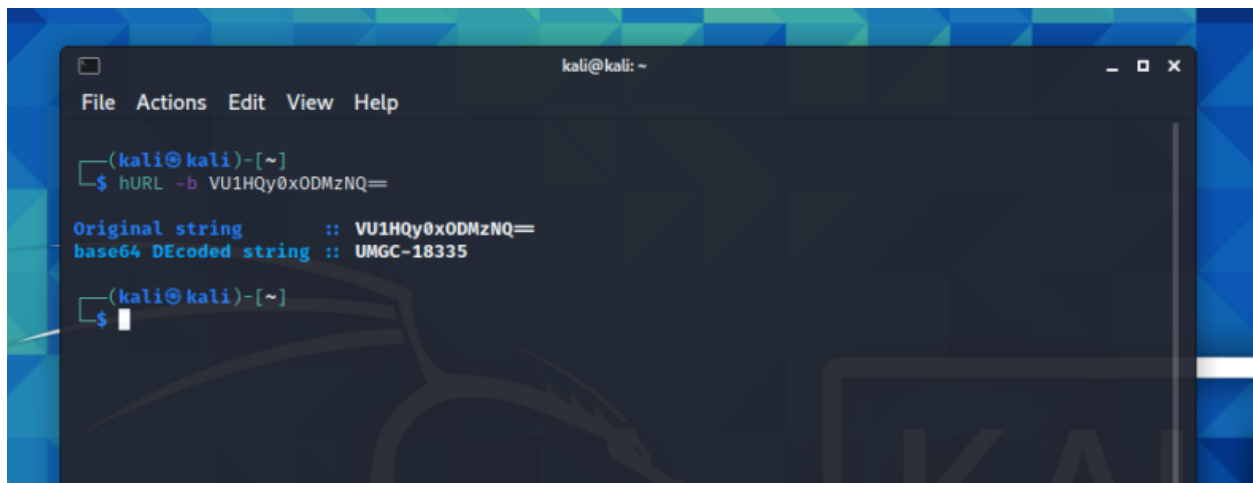


Section I: The Solves

I attempted the first challenge in each of the first nine categories. After that I tried a few extra challenges among the encryption and password challenges.

Section II: Strategies Employed

For the Category 1 challenge 1, I used a program on Kali Linux called “hURL.” hURL is a basic encoder/decoder that can be installed in Kali Linux (fnord0, 2021). In the terminal window go to the root directory using `cd` and then type `hURL -b VU1HQy0xODMzNQ==`. This produces the output `UMGC-18335` which is the flag for this challenge.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ hURL -b VU1HQy0xODMzNQ==  
Original string      :: VU1HQy0xODMzNQ==  
base64 DEcoded string :: UMGc-18335  
(kali@kali)~  
$
```

Figure 1: Category 1 Challenge 1 Solved

For Category 6 Challenge 1, I used WireShark (WireShark, 2021) to view the capture file. After bringing up the file, I used the filter to look for “SSH” which produced the output below. Highlighted in red, you can see where the SSH filter is, two instances of the IP Address (192.168.1.200), and the target server’s information.

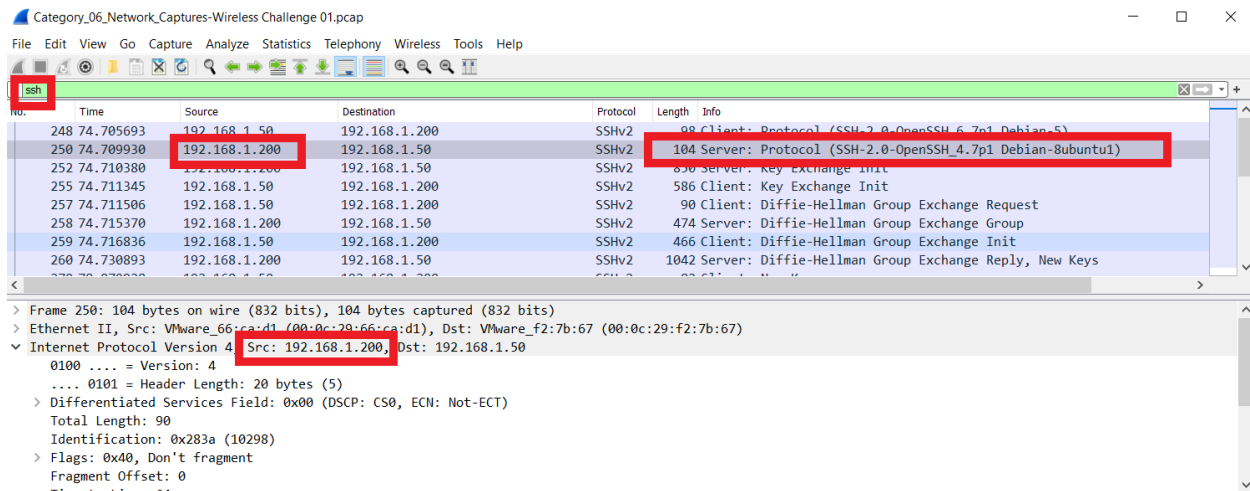


Figure 2: Capture file output with filter, IP Address, and server information high-lighted

Section III: Lessons Learned

- Right now, my strengths involve information gathering through open-source information systems. Until I get more experience in the other categories, I think a CTF team would benefit most from my ability to find information quickly and easily.
- The challenge banks that I found easiest, were the Open-Source Intelligence and Log Analysis challenges. I am new to hacking and the methods involved, so the more technical challenges are difficult for me, but these two areas involve research and finding information. I have plenty of experience in both areas which helped finish these with greater ease.
- I need more practice analyzing files and finding information that is not readily available on open sources. I also need to get better at knowing what tools I need to use for specific tasks.
- I avoided Category 10 since it required a large download and my internet capabilities are very limited in my current location.
- Three challenges that I have not completed yet are Category 2 Challenge 1, Category 3 Challenge 1, and Category 5 Challenge 1.
 - Category 2 I was able to half complete, I found the actual file extension, but I am having trouble finding the exact name of the file. I do not know if I am over thinking it and the name is the same as the file that is originally downloaded.
 - Category 3 I have found a few different methods to get information out of the registry files, but I have not found out how to get the IPV4 address yet.
 - Category 5 I initially tried reading the files through 7zip, but I think I need to use a different tool to analyze the malware.
- The best way to improve my skills in these areas is to know what tools I need to use and how to use them to find the information I want. As I progress, and learn more about hacking methods and tools, I will likely find some of these challenges are not as hard as they currently seem to be.

References

fnord0. (2021). *hurl Package Description*. Retrieved from Kali Tools: <https://tools.kali.org/web-applications/hurl>

WireShark. (2021). *WireShark*. Retrieved from WireShark: <https://www.wireshark.org/>