



Capture The Flag

NAME: RALPH RODRIGUEZ

TEAM NAME: OMEGA RED

Introduction

- The CTF Problem
- Introduction to the Problem
- Working Toward a Solution
- Arriving at The Solution
- Strategies, Pitfalls, Lessons Learned
- Workplace Relevance
- Summary
- Demo

CTF The Problem :

CHALLENGE 6: USE THE CAPTURE FILE PROVIDED TO DETERMINE DARTH VADER'S PASSWORD.

- Passwords are often misplaced or forgotten — even by high-profile users.
This challenge simulates a realistic scenario where recovering a lost password is critical.
- We explore a fast and effective recovery method using forensic tools.
By analyzing network traffic from a capture file, we extract key data in just minutes.

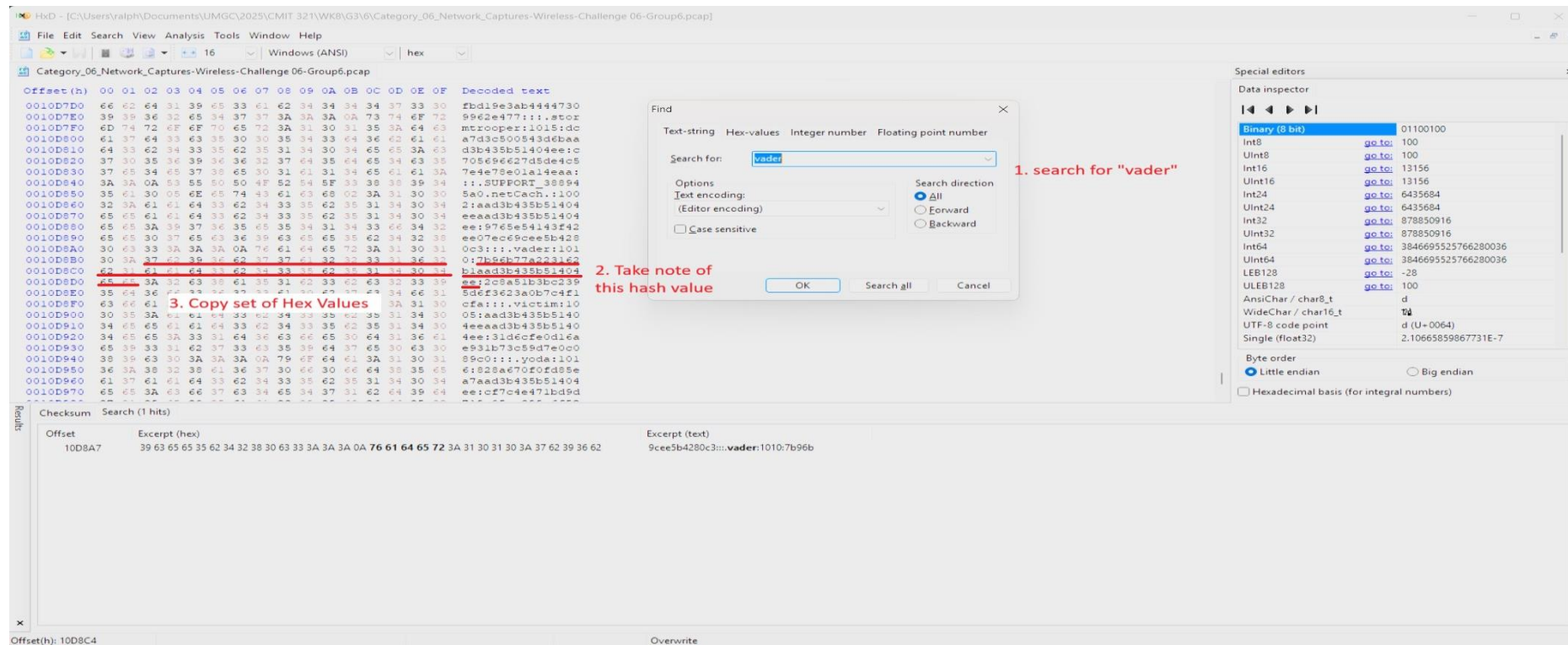
CTF The Problem :

CHALLENGE 6: USE THE CAPTURE FILE PROVIDED TO DETERMINE DARTH VADER'S PASSWORD.

EXECUTION FLOW

- PACKET ANALYSIS
- HASH EXTRACTION
- PASSWORD RECOVERY

Introduction to the Problem



- With a Hex editor open the PCAP file and search for "Vader"
- Take note of the HASH value and copy the HEX values

Working Toward A Solution

The image shows two windows side-by-side. The left window is HxD, a hex editor, displaying a file named 'Category_06_Network_Captures-Wireless-Challenge 06-Group6.pcap'. It shows a list of hex values and their corresponding ASCII characters. The right window is Wireshark, displaying the same file. It shows a list of network packets and their details. A red box highlights a specific packet (No. 1314) and its details (Frame 9968: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits) on Ethernet II, Src: VMware_e0:09:3f (00:0c:29:e0:09:3f), Dst: VMware_64:0f:98 (00:0c:29:64:0f:98)). A red box also highlights the packet's details (Internet Protocol Version 4, Src: 192.168.1.175, Dst: 192.168.1.101). A red box highlights the packet's details (Transmission Control Protocol, Src Port: 1181, Dst Port: 4444, Seq: 173, Ack: 311949, Len: 1260). A red box highlights the packet's details (Data [1260 bytes]). A red box highlights the packet's details (Data [1260 bytes]). A red box highlights the packet's details (Data [1260 bytes]).

3. Set this to Hex Value

4. Press ctrl-F, paste HEX value from HxD, and search

5. Copy both Hash values onto your notepad. Make sure to keep them separated.

- Open the same file with Wireshark & search for the same HEX value
- Verify the same HASH value from the left (HxD) are the same as with the ones on the right (Wireshark)
- Copy the 2 HASH values from Wireshark

Arriving at the Solution

- Open a web browser and visit crackstation.net
- Paste each HASH value on a separate line, complete the CAPTCHA, and click "Crack Hashes"
- Navigate to the results column and the answer: "red"

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links like 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below this, there's a text input area where two hashes are pasted: '7696b77a223162b1a4d3043951404ce' and '2c8a5183bc2395d6f3623a0b7c4f1cfa'. A red box highlights the input area with the instruction '6. Paste each HASH on a separate line'. To the right of the input area is a CAPTCHA challenge with the text 'I'm not a robot' and a 'CAPTCHA' button. A red arrow points to the CAPTCHA button with the instruction '7. Complete CAPTCHA and Crack Hashes'. Below the input area, there's a table with three columns: 'Hash', 'Type', and 'Result'. The table contains 10 rows of data. The first 9 rows have a 'Type' of 'MD5' and a 'Result' of 'Not found'. The 10th row has a 'Type' of 'MD5' and a 'Result' of 'red'. A red arrow points to the 'red' result with the instruction '8. CTF Answer: "red"'. Below the table, there's a 'Download CrackStation's Wordlist' link. At the bottom, there's a 'How CrackStation Works' section with a brief explanation of the service. The website footer includes a 'Defuse.ca' link and a Twitter icon.

| Hash | Type | Result |
|----------------------------------|------|-----------|
| 7696b77a223162b1a4d3043951404ce | MD5 | Not found |
| 2c8a5183bc2395d6f3623a0b7c4f1cfa | MD5 | Not found |
| 7696b77a223162b1a4d3043951404ce | MD5 | Not found |
| 2c8a5183bc2395d6f3623a0b7c4f1cfa | MD5 | Not found |
| 7696b77a223162b1a4d3043951404ce | MD5 | Not found |
| 2c8a5183bc2395d6f3623a0b7c4f1cfa | MD5 | Not found |
| 7696b77a223162b1a4d3043951404ce | MD5 | Not found |
| 2c8a5183bc2395d6f3623a0b7c4f1cfa | MD5 | Not found |
| 7696b77a223162b1a4d3043951404ce | MD5 | Not found |
| 2c8a5183bc2395d6f3623a0b7c4f1cfa | MD5 | red |

Strategies, Pitfalls, Lessons Learned

- **Faster Strategy:**

The hash can be copied directly from the hex editor (HxD) and submitted to CrackStation without needing Wireshark — saving time.
- **Common Pitfall:**

Since the file is a .pcap, it's natural to open it in Wireshark first. However, searching for "vader" in Wireshark doesn't return useful results — HxD is more effective in this case.
- **Lesson Learned:**

It's important to understand the strengths and limitations of both Wireshark and HxD. Choosing the right tool for the task makes a big difference in solving CTF challenges efficiently.

Workplace Relevance

- **Real-World Packet Analysis:**

Skills in analyzing .pcap files using tools like Wireshark and hex editors are directly applicable in incident response and threat hunting.

- **Hash Recognition and Cracking:**

Understanding how to identify and crack password hashes helps with password auditing, penetration testing, and verifying credential leaks.

- **CTF Practice = Hands-On Readiness:**

Capture the Flag (CTF) challenges simulate real cybersecurity problems, building muscle memory for tasks like data extraction, protocol analysis, and threat detection.

Summary

In these challenges, I successfully extracted and cracked a password from a .pcap file using a combination of HxD (hex editor) and online tools. Although Wireshark is a go-to tool for packet analysis, this scenario highlighted the importance of choosing the right tool for the task. HxD provided a more direct path to the solution. I learned that understanding how to navigate raw data, identify hashes, and use external resources like CrackStation can significantly speed up problem-solving. This hands-on exercise not only strengthened my technical skills but also deepened my understanding of packet-level data analysis, which is highly relevant in cybersecurity roles such as threat analysis, digital forensics, and penetration testing.