Befund

Spongebob Squarepants lost the password to his Veracrypt container. The container was provided as part of the assignment and contained three images featuring Spongebob as well as a text file titled secret.txt. The following factual details summarize the procedure and results of the investigation.

Container Analysis

Name: *container_12439010.hc*

SHA-256 (before investigation):

9fc8386f7d9ddd01314064add08e1e3b231a8077ac3a306c5618aa02a9d8d192

Content Found:

- three images showing Spongebob Squarepants
- file named *secret.txt* containing the string:

“7435b0be2c634533a2420cb3e0b53e70e66f4c32f7”

Password Cracking Process

Hardware Used: NVIDIA RTX 4070 LAPTOP GPU

Software Tool: Hashcat

Hash Mode: 13711 (VeraCrypt RIPEMD160 + XTS 512 bit (legacy)

Cracking Command:

```
hashcat -m 13711 -a 3 -d 1 -w 4 -S -O container_12439010_digits4.hc ?d?d?d?d
```

Execution Details

Start Time: Thu Apr 3 20:07:31 2025

Duration: Approximately 25 seconds

Password Space: 10,000 combinations (numeric, 4 digits)

Cracked Password: 4473

Hashcat result message:

```
container_12439010_digits4.hc:4473
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13711 (VeraCrypt RIPEMD160 + XTS 512 bit (legacy))
Hash.Target......: container_12439010_digits4.hc
Time.Started.....: Thu Apr  3 20:07:31 2025 (25 secs)
Time.Estimated...: Thu Apr  3 20:07:56 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?d?d?d?d [4]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 405 H/s (4.31ms) @ Accel:1024 Loops:500 Thr:512 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10000/10000 (100.00%)
Rejected.........: 0/10000 (0.00%)
Restore.Point....: 5000/10000 (50.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:655000-655330
Candidate.Engine.: Host Generator + PCIe
Candidates.#1....: 1236 -> 6883
Hardware.Mon.#1..: Temp: 60c Util: 93% Core:2460MHz Mem:8001MHz Bus:8
Started: Thu Apr  3 20:07:08 2025
Stopped: Thu Apr  3 20:07:57 2025
```

No errors or rejections were encountered during the run.

SHA-256 (after investigation):

9fc8386f7d9ddd01314064add08e1e3b231a8077ac3a306c5618aa02a9d8d192

Gutachten

Analysis of Brute-Force Requirements

Time Estimates for Various Password Complexities.

4-Digit Numeric Passwords:

Total combinations: 10,000

With the current setup (NVIDIA RTX 4070 Laptop GPU and optimized Hashcat parameters), a 4-digit numeric password was cracked in roughly 25 seconds.

Increasing Password Lengths and Complexity.

6-Digit Numeric Passwords:

1,000,000 combinations – time scales linearly with the number of guesses, which could extend the cracking time significantly under similar conditions.

Alphanumeric or Mixed-Character Sets:

Inclusion of both uppercase and lowercase letters, digits, and symbols dramatically increases the search space. For example, a 6-character password using 62 possible characters has over 56 billion combinations.

The required brute-force time increases exponentially with password length and complexity. Therefore, while a 4-digit PIN can be brute-forced in seconds, longer and more complex passwords would require orders of magnitude more time even on high-end GPUs.

Recommendations for 10-Year Secure Containers

To achieve security over a period of 10 years, it is essential to select a password with a high level of entropy.

Minimum Recommendation:

A password of at least 12 characters that includes a mix of lowercase letters, uppercase letters, digits, and special symbols.

Rationale:

A 12-character password with a full set of 94 printable characters provides a search space of approximately $4.7 * 10^{23}$ combinations. This vast search space is currently beyond the practical reach of brute-force methods using standard hardware—even with state-of-the-art GPUs.

Conclusion

The investigation successfully recovered the container password (‘4473’) using a GPU-accelerated brute-force attack with Hashcat. The container's contents included three images of Spongebob Squarepants and a secret file with a hash value. Our analysis confirms that for long-term security (e.g., 10 years), significantly stronger and more complex passwords (12 characters with mixed sets) are required to withstand modern brute-force techniques.