Paul Badu Yakubu

Penetration Testing

Prof. Anthony J Candeias

March 11, 2024

NCL Writeup

For the National Cyber League (NCL) password cracking challenge involved attempting to crack a series of password hashes using the Rockyou wordlist, a massive compilation of commonly used passwords obtained from various data breaches. I was are provided with a set of password hashes, which are cryptographic representations of passwords. These hashes are generated using hash algorithms like MD5 making it computationally infeasible to reverse the process and obtain the original passwords directly.

To crack these password hashes, I used password cracking tools such as hashcat, configuring it to perform dictionary attacks with the Rockyou wordlist. In a dictionary attack, the password cracking tool iterates through each entry in the wordlist, hashing each word and comparing it against the provided password hashes. If a match is found, indicating that the hashed word corresponds to one of the passwords in the wordlist, the tool successfully cracks the password.

The provided command demonstrates how to use hashcat, a popular password-cracking tool, to crack password hashes using a dictionary attack with the Rockyou wordlist. Here's a detailed explanation of each component of the command:

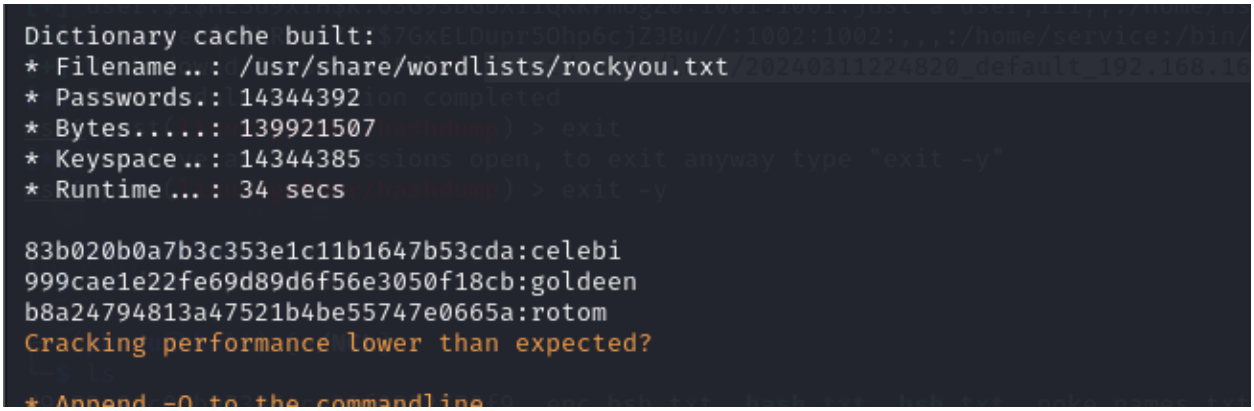
```
hashcat hash.txt -m 0 -a 0 /usr/share/wordlists/rockyou.txt
```

1. *hashcat*: This is the name of the password cracking tool being used. Hashcat is a powerful and fast password recovery utility that supports various hash algorithms and attack modes.

2. *hash.txt*: This is the file containing the password hashes that you want to crack. The hashes can be stored in a text file, with each hash on a separate line. Hashcat will read these hashes from the specified file and attempt to crack them.
3. *-m 0*: This option specifies the hash type or algorithm used to hash the passwords. In this case, the value 0 indicates that the hashes are MD5 hashes. Hashcat supports a wide range of hash types, each identified by a unique numerical value.
4. *-a 0*: This option specifies the type of attack to perform. In this case, the value 0 indicates a dictionary attack. A dictionary attack involves attempting to crack passwords by comparing them against a list of words from a dictionary or wordlist.
5. */usr/share/wordlists/rockyou.txt*: This is the path to the wordlist file that contains the list of words or passwords to use in the dictionary attack. The Rockyou wordlist is a commonly

used wordlist included by default in Kali Linux, located in the specified directory. It contains millions of commonly used passwords and is often used in password cracking exercises due to its extensive coverage.

By running the provided command, hashcat will use the specified MD5 hashes from the hash.txt file and attempt to crack them using the dictionary attack method, comparing them against the passwords in the Rockyou wordlist. If any of the hashes match a password in the wordlist, hashcat will successfully crack the password and display it as the output. This process allows security professionals to assess the strength of passwords and identify any weak or easily guessable passwords that may need to be strengthened for improved security.



Hashcat could crack all three password hashes I provided as input. This indicates that the passwords were weak and vulnerable.
