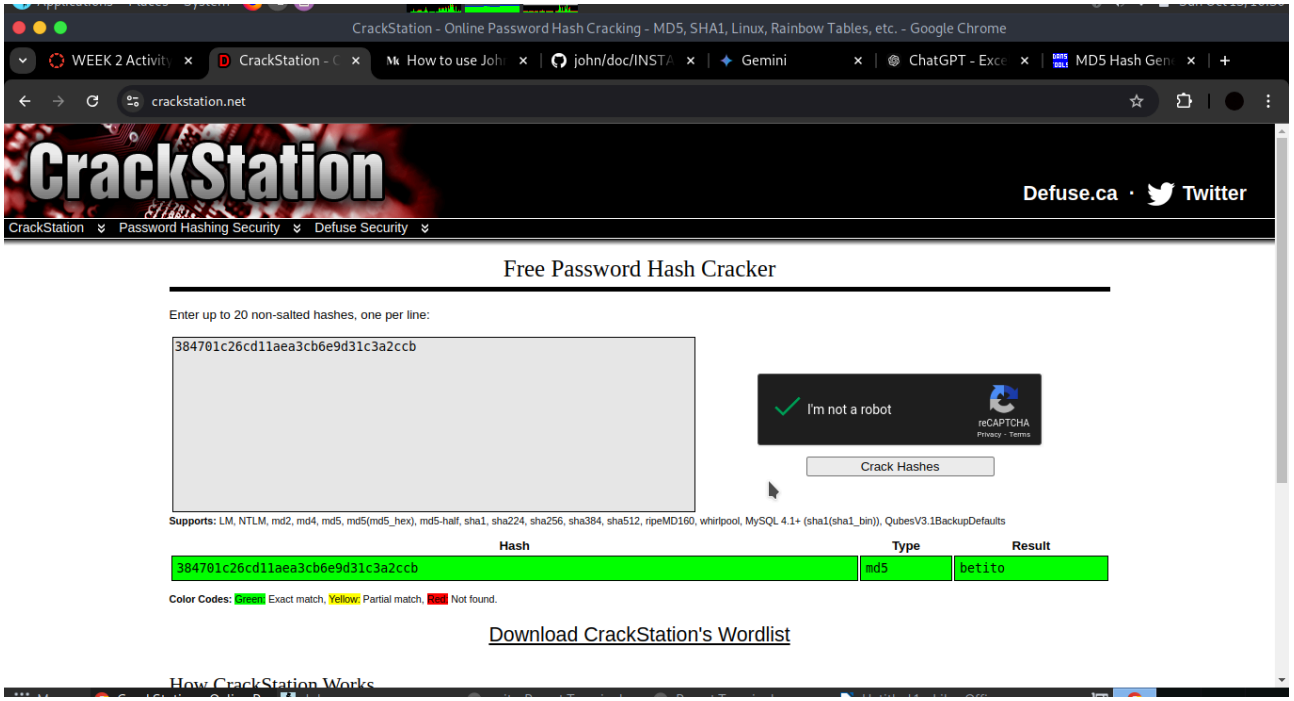
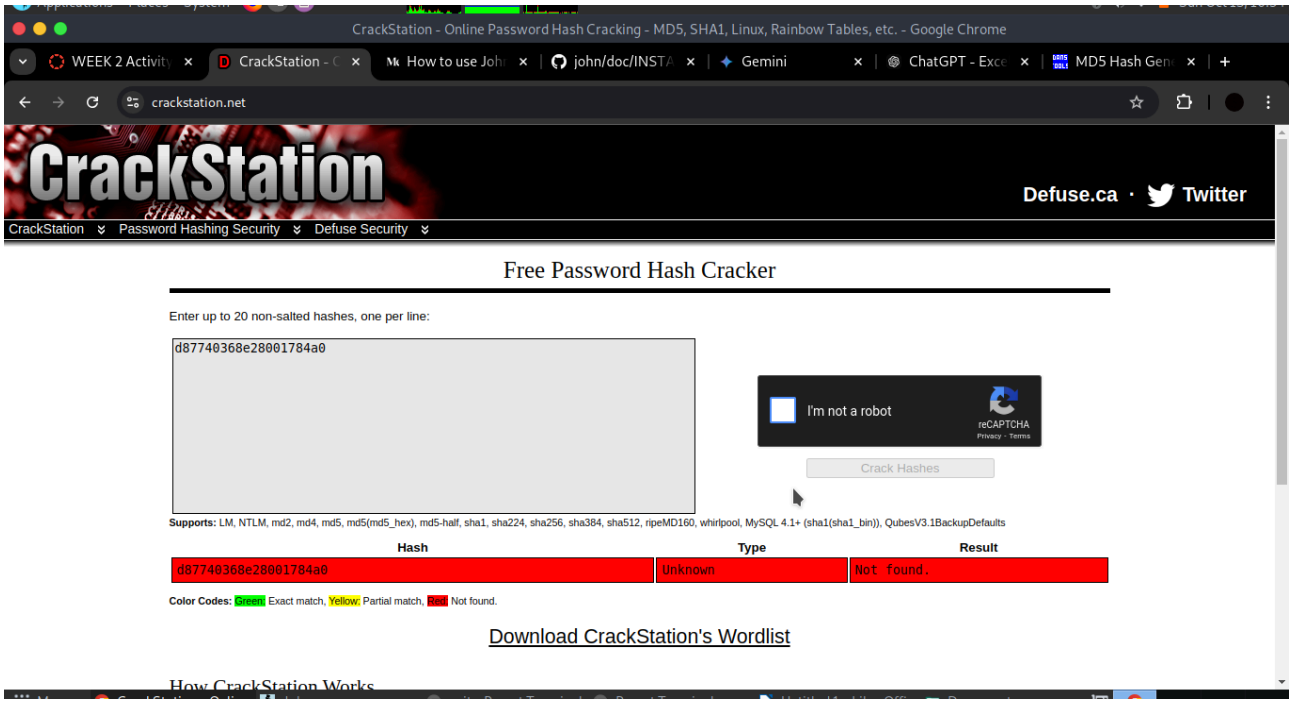
PASSWORD CRACKING

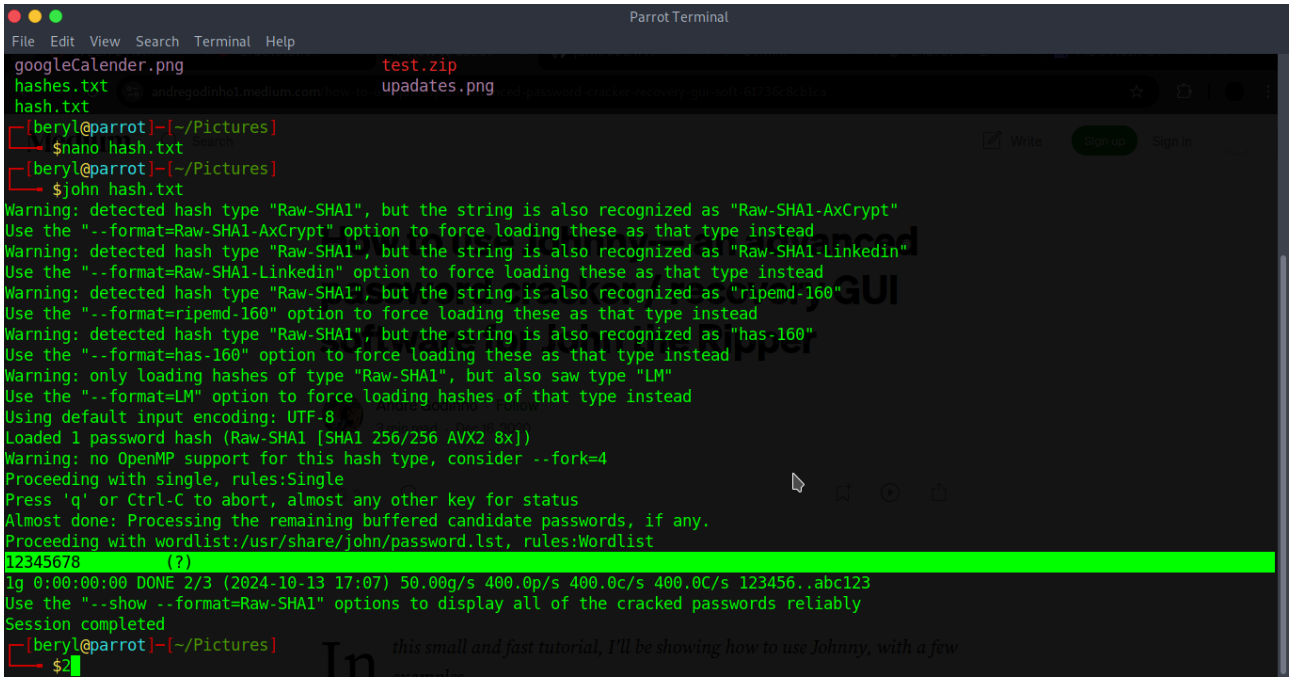
Password cracking is the process of attempting to recover a password from its encrypted form. In this report, I used John the ripper and crack-station as our cryptographic attack tools. Crack-station is an online password cracking service that allows users to submit password hashes for cracking. It provides information about the password's strength and potential matches from its extensive database. Crack-station allow hashes in SHA variants such as sha1, sha224, sha256, sha384, sha512. It also allows MD5 variants that include MD5LM, NTLM, md2, md4, md5, md5(md5_hex) and md5-half. Additionally, it gives room for other algorithms like ripeMD160, whirlpool and MySQL 4.1+ LM. I started with a weak password which was hashed in MD5 format and it only took crack-station microseconds to crack the password.



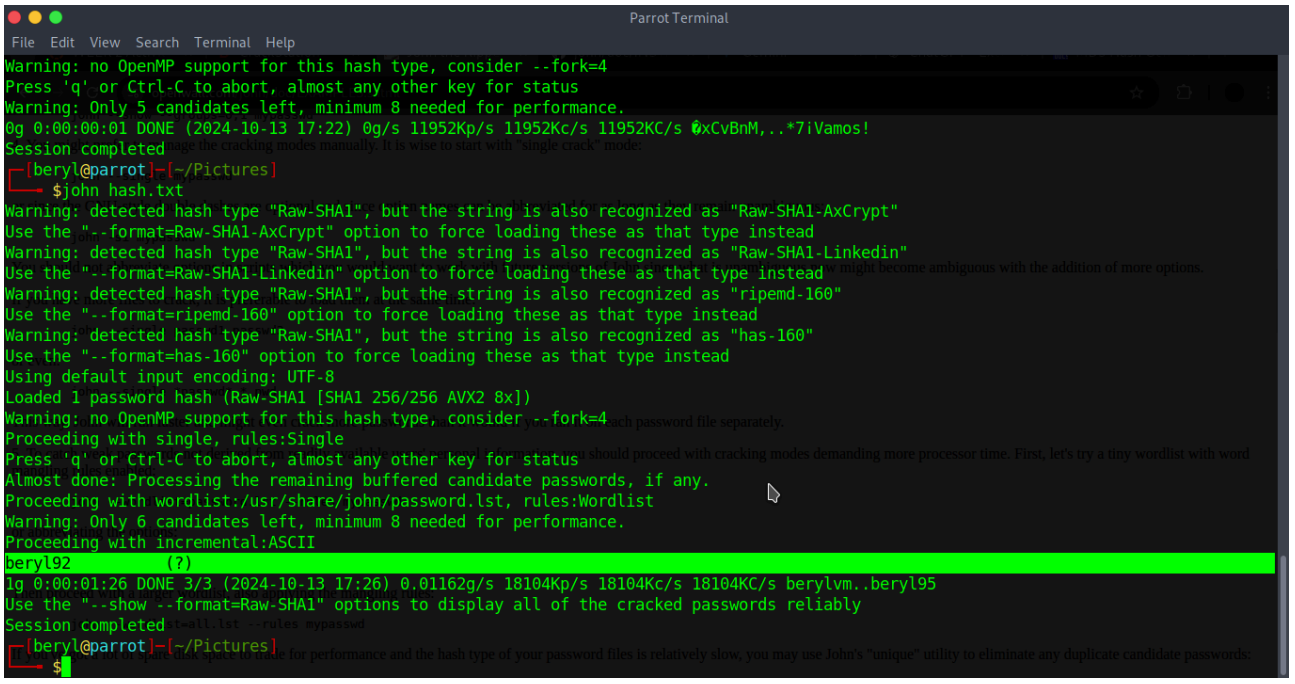
I tried cracking a complex password using special characters, numbers, capital letters and small letters. Crack-station could crack the password. Crack-station could not crack password hashes which were in yescrypt format since yescrypt format is more complex to crack or brute-force. The shorter the password the shorter the time used to crack.



I stored two hashed passwords on a hash.txt file and used john the ripper to crack the password. John cracked on a simple password which was in sha1 format.

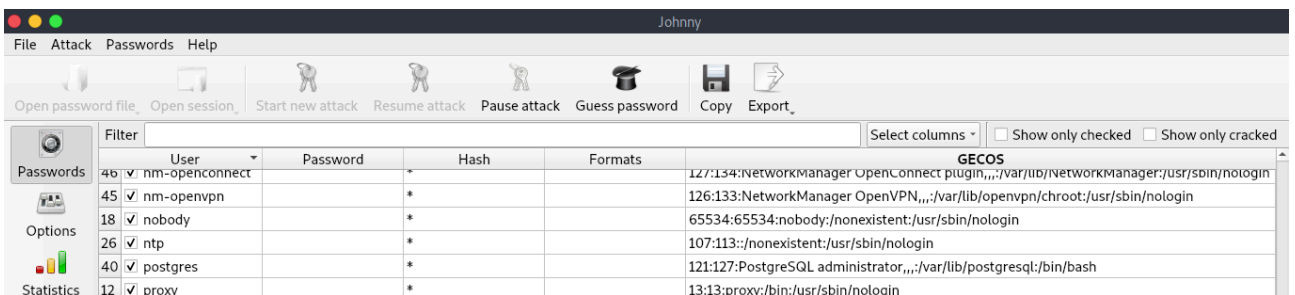


While trying a more complex password, john the ripper took long to output the results.

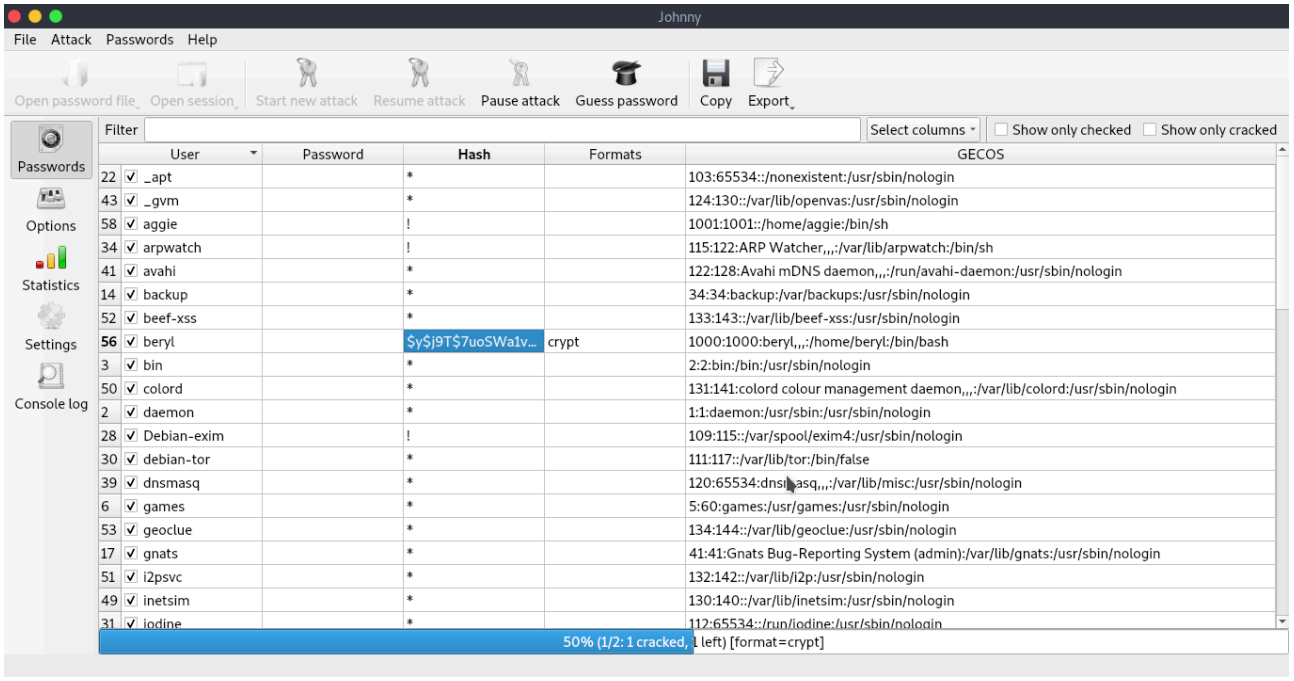


The systems password stored in my etc/shadow were in a yescrypt hash format which is hard to crack using john the ripper unless I use john-jumbo.

Parrot os had a GUI interface for john the ripper called johnny which is easier to use than the terminal. It automatically identifies the has format for a particular password. In this case I uploaded a file containing all my hashed passwords that are in my etc/shadow file.



Jonny used wordlists and cracked the weakest password for my root user in seconds. The tool was designed to be intuitive and accessible, even for users who are not experienced with password cracking. The interface is straightforward, and the tool provides clear instructions and error messages. Additionally, John the Ripper offers a wide range of options and configurations, allowing users to customize the tool to their specific needs.



Since user beryl has a complex password I had to cancel the process because it took forever to crack the password.

To prevent brute-force attacks, one needs to use complex passwords which are a combination of uppercase, lowercase letters, numeric numbers and special characters. This makes it difficult for an attacker to brute-force the correct password. Longer passwords are encouraged because longer passwords are more difficult to crack. Furthermore one is encouraged to avoid common words and that can be quickly discovered in a dictionary attack. Ideally, using password managers can help create and store passwords.

In summary, strong passwords and encryption are essential tools to protect against brute force attacks and other security threats. By using complex, unique passwords and implementing encryption, you can significantly reduce the risk of unauthorized access to your systems and data.