Commands from the SANS Password Cracking for OSINT and Digital Forensics Workshop by Matt Edmondson @Matt0177

Extracting Hashes:

To extract the hash from a zip file:

/snap/john-the-ripper/581/run/zip2john ~/Desktop/workshop/file.zip

To save the hash to a text file:

/snap/john-the-ripper/581/run/zip2john ~/Desktop/workshop/file.zip > ziphash.txt

To extract the hash from a rar file:

/snap/john-the-ripper/581/run/rar2john ~/Desktop/workshop/file.rar

To save the hash to a text file:

/snap/john-the-ripper/581/run/rar2john ~/Desktop/workshop/file.rar > rarhash.txt

To extract the hash from an Office document:

python3 /snap/john-the-ripper/581/run/office2john.py ~/Desktop/workshop/modern_excel_pw.xlsx

To save the hash to a text file:

python3 /snap/john-the-ripper/581/run/office2john.py ~/Desktop/workshop/modern_excel_pw.xlsx > officehash.txt

To extract the hash from a PDF file:

/snap/john-the-ripper/581/run/pdf2john.pl ~/Desktop/workshop/wizard.pdf

To save the hash to a text file:

/snap/john-the-ripper/581/run/pdf2john.pl ~/Desktop/workshop/wizard.pdf > pdfhash.txt

Cracking Hashes:

To crack RAR hash:

hashcat -m 13000 rar_hashcat.txt ~/Desktop/workshop/password.lst

To crack Office hash file:

hashcat office_hashcat.txt -m 9600 ~/Desktop/workshop/password.lst

To crack Zip hash:

hashcat hashcat_zip.txt -m 13600 ~/Desktop/workshop/password.lst

To crack PDF hash:

hashcat -m 10500 pdf_hashcat.txt ~/Desktop/workshop/password.lst

To crack a zip hash using the dictionary and a rule set:

hashcat rulehash.txt -m 13600 ~/Desktop/workshop/password.lst ***-r /usr/share/hashcat/rules/dive.rule***

Resources:

https://www.digitalforensicstips.com/

https://www.openwall.com/john/

https://hashcat.net/hashcat/

https://www.grc.com/haystack.htm

https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm

https://hashcat.net/wiki/doku.php?id=example_hashes

https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt