Refog, Spyrix, John the Ripper, or Prey

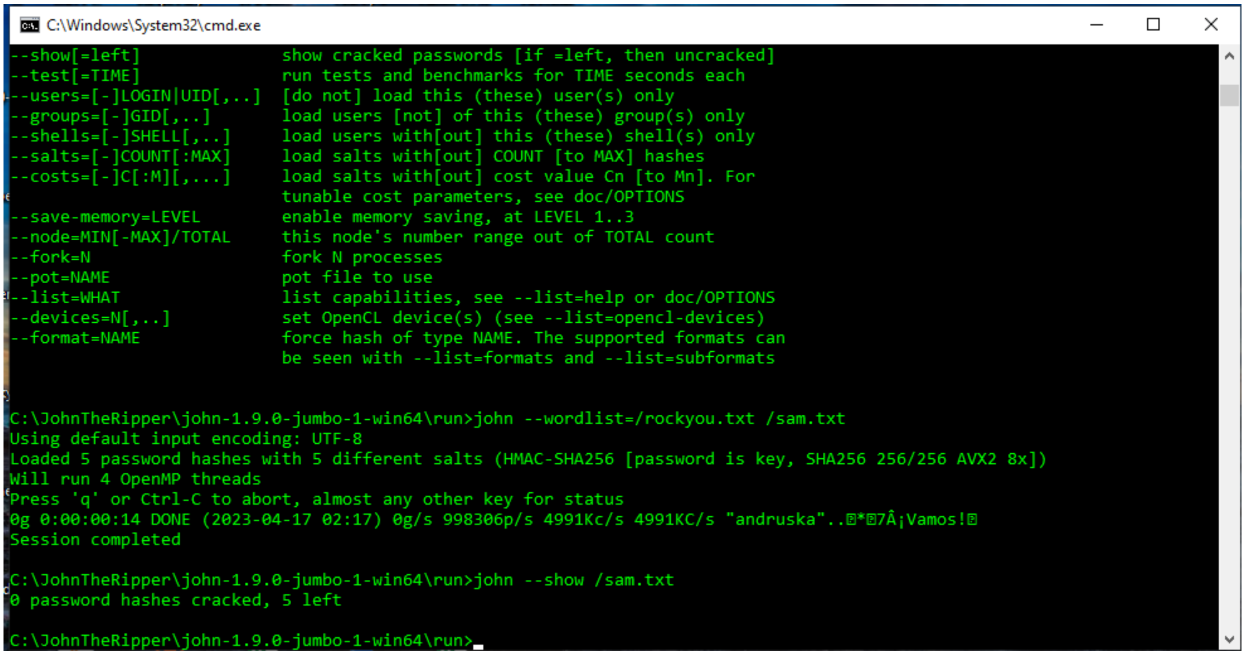
What I Did

For John the Ripper, I downloaded the john 1.9.0-jumbo-1 64-bit Windows version. Then, I researched how to install John the Ripper on Windows and followed the "How to Install John the Ripper on Windows?" tutorial at https://www.geeksforgeeks.org/how-to-install-john-the-ripper-on-windows/. The tutorial stated to unzip the john-1.9.0-jumbo-1-win64 folder, add a folder named JohnTheRipper to the C drive, cut and paste the files from the john-1.9.0-jumbo-1-win64 folder to the new JohnTheRipper file, open the Run folder, open the command prompt with the Run folder, and type "john" and press enter to verify that John the Ripper is running properly (GeeksforGeeks, 2021). I completed all of the steps. I had trouble moving some of the documents to the C drive. I just kept pressing the try again option, and the folders were eventually successfully moved over. Then, I began researching how to select a wordlist and run it against my own machine to see how many passwords could be cracked. I found out about rockyou.txt, which is a wordlist of common passwords, the SAM database, which is the database for password hashes in Windows, and the commands to run for dictionary mode on John the Ripper, which were "john --wordlist=/rockyou.txt /sam.txt" and "john –show /sam.txt" on the command prompt (Shivanandhan, 2022). Then, I downloaded the rockyou wordlist text file from GitHub at https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt and cut and pasted it to the JohnTheRipper file on the C drive. I watched a video describing how to copy the SAM file. The video explained to open the administrator command prompt and run the command "reg save hklm\sam c:\sam" to save the sam file in the C drive. (SoftwareGeek, 2017). I followed the directions and moved the sam file to the desktop, opened it with Notepad, saved it as sam.txt, and cut and pasted it to the JohnTheRipper file. I tried to run the command "john --wordlist=/rockyou.txt /sam.txt" using the command prompt with the run folder and got a warning about the rockyou.txt and sam.txt files not being completely in UTF-8 format. So, I copied them to the desktop. I opened the files with Notepad, resaved both with the encoding option set to UTF-8, and cut and pasted the files into the JohnTheRipper file on the C drive. Then, I tried to run the command "john --wordlist=/rockyou.txt /sam.txt" and got the error "open: john.log: Permission denied." So, I changed the security properties for the JohnTheRipper file to be able to modify and write to necessary documents. Finally, I ran the commands of "john --wordlist=/rockyou.txt /sam.txt" and "john –show /sam.txt" and got outputs without any error messages. Then, I deleted the JohnTheRipper file, including the rockyou.txt and sam.txt files. I used CCleaner to permanently remove them from my computer.

For Prey, I downloaded Prey Free on my phone, target machine and set up and activated my account. My target machine started sending signals to the control machine. I completed a test report, which showed me a sample report on my target machine of what I would be able to generate using the control machine, if I were to set my device to missing online, using my account. I continued to use Prey to track my phone's location online through GPS, Wi-Fi triangulation, and GeoIP signals sent from my phone (*Laptop Tracking Solution: Track and Find Laptops & Other Mobile Devices*, n.d.). Then, I tried to uninstall the app off of my phone, target machine to see what would happen and tried turning off my phone, target machine to see what would happen.

What Are My Results

My results for John the Ripper can be seen below in Figure 1.



```
--show[=left]              show cracked passwords [if =left, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]     load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]     load salts with[out] cost value Cn [to Mn]. For
                           tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--devices=N[,..]           set OpenCL device(s) (see --list=opencl-devices)
--format=NAME              force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats


C:\JohnTheRipper\john-1.9.0-jumbo-1-win64\run>john --wordlist=/rockyou.txt /sam.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:14 DONE (2023-04-17 02:17) 0g/s 998306p/s 4991Kc/s 4991KC/s "andruska"..*7Â¡Vamos!
Session completed

C:\JohnTheRipper\john-1.9.0-jumbo-1-win64\run>john --show /sam.txt
0 password hashes cracked, 5 left

C:\JohnTheRipper\john-1.9.0-jumbo-1-win64\run>
```

Figure 1: Input and Output for John the Ripper

First, the tool detected the encoding for rockyou.txt as UTF-8. Then, John the Ripper found five password hashes, using five different salts in sam.txt. Password hashes are passwords that have been put through a hashing algorithm to generate "an unintelligible series of numbers and letters," and salts are "a series of random characters" added to a password before using a hashing algorithm (Jung, 2021). Then, the tool tried to crack the password hashes in sam.txt, using the wordlist rockyou.txt. None of the 5 passwords for my machine were cracked.

For Prey, the results of the test report included the current latitude, longitude, SSID, public IP address, device model name, view from front camera, view from back camera, and location on Google Maps of my phone, the target machine. I can log in online from anywhere to track my phone with an accuracy of 11 to 12 meters. When, I tried to delete the app off of my phone, a message came up that stated, "Uninstalling Prey unsuccessful. Can't uninstall active device admin app." My phone, target machine continued to send signals to the control machine. When I turned off my phone, the target machine's location became unreachable because signals could no longer be sent to the control machine.

What Did I Learn

While trying to figure out John the Ripper, I learned more about files in the C drive, the command prompt, the administrative command prompt, the SAM database, how to make a copy of the sam file, hashing, and salting. Also, I learned how to use John the Ripper at a beginner level. Also, I completely deleted John the Ripper off of my laptop, so it is not ready to be used by anyone trying to attack my laptop. I will not be allowing people access to my computer. I'm sure there are many different tools that people could use to attack devices that I wouldn’t even know to look for on my laptop. I will keep up with the updates on my computer, too.

While using Prey, I learned how devices can be tracked with GPS, Wi-Fi triangulation, and GeoIP signals. I was surprised how the software could even depict an accurate location of my phone, when I just moved it to different rooms in my home. Prey would probably be good for monitoring kids, but it could be bad, if someone installed it on a person’s phone without that person knowing and used it to track them to their home or somewhere else. Advances in technology can help people, but they can create vulnerabilities, too.

References

GeeksforGeeks. (2021). How to Install John the Ripper on Windows. *GeeksforGeeks*. https://www.geeksforgeeks.org/how-to-install-john-the-ripper-on-windows/

Jung, J. (2021, May 7). What are Salted Passwords and Password Hashing? *Okta, Inc.* https://www.okta.com/blog/2019/03/what-are-salted-passwords-and-password-hashing/#:~:text=Password%20hashing%20is%20defined%20as,unintelligible%20to%20the%20bad%20actor.

Laptop Tracking Solution: Track and find laptops & other mobile devices. (n.d.). https://preyproject.com/features/tracking-and-location

Shivanandhan, M. (2022). How to Crack Passwords using John The Ripper – Pentesting Tutorial. *freeCodeCamp.org*. https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/

SoftwareGeek. (2017, April 5). *How to copy SAM file and SYSTEM file with CMD* [Video]. YouTube. https://www.youtube.com/watch?v=XN3NNk93C_U