

### **Introduction:**

John the Ripper is an open source software tool for cracking passwords. It often creates rainbow tables/dictionaries of hashed passwords. This software can run on over 15 different platforms. This report will go over the installation and configuration process of John the Ripper on a Google Virtual Machine. Following, a walkthrough is provided on using the software to crack a password from a file downloaded from a server.

### **Installation:**

After opening up the Google VM, the first necessary command to run is, *sudo apt install gcc build-essential git zlib1g-dev libssl-dev*. After this command has finished running, the next command to use is, *git clone <https://github.com/magnumripper/JohnTheRipper>*. Proceeding, it's necessary to move into the correct directory. This prompts the command, *cd JohnTheRipper/src* to be used. The following steps involve the configuration process of the software; first run, *./configure*, following enter the command *make*, which takes several minutes. Lastly enter, *make install*. The VM should now be all set up to use John the Ripper. To ensure that the software has been properly installed, change directories to JohnTheRipper/run, and enter the command, *./john*.

### **Downloading rockyou.txt:**

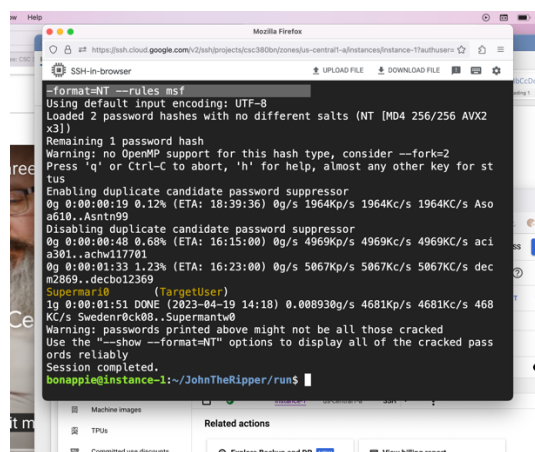
Rockyou.txt is a file that contains millions of possible passwords in plaintext form. To download this file to the VM, enter the command, *wget <http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2>*, in the JohnTheRipper/run directory. Rockyou.txt will initially download as a zip file, so

after the download completes, it will be necessary to run the command, *bunzip rockyou.txt.bz2*, to unzip it.

### **Walkthrough: Cracking a Password:**

Working in the directory, *JohnTheRipper/run*, to crack a password found within a downloaded file, run the command, *./john* (this runs the John The Ripper software). In the proper format, the code would look something like, *./john --wordlist=rockyou.txt --format=NT --rules pass*. Replace “*pass*” with the name of the file that contains passwords to be cracked.

Still working in the directory, *JohnTheRipper/run*, the file, *msf.txt* was downloaded from the system administrators server by utilizing the command, *wget http://192.168.\*\*\*\*/admin/msf.txt*. I took the contents of *msf.txt* and printed it to a file called *msf*. From here I used the command, *./john --wordlist=rockyou.txt --format=NT --rules msf*, to find the password of TargetUser. The revealed password was, *Supermario0*. A note, “*--rules*” is important to include in the command, as it accounts for users implementing a combination of uppercase, lowercase, and numbers in their passwords. Below is an image of the output containing the decrypted password.



```

format=NT --rules msf
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2
x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for st
tus
Enabling duplicate candidate password suppressor
0g 0:00:00:19 0.12% (ETA: 18:39:36) 0g/s 1964Kc/s 1964Kc/s Aso
a610..Asntng9
Disabling duplicate candidate password suppressor
0g 0:00:00:48 0.68% (ETA: 16:15:00) 0g/s 4969Kc/s 4969Kc/s aci
a301..achw117781
0g 0:00:01:33 1.23% (ETA: 16:23:00) 0g/s 5067Kc/s 5067Kc/s dec
m2869..decbo12369
Supermario0 (TargetUser)
1g 0:00:01:51 DONE (2023-04-19 14:18) 0.008930g/s 4681Kc/s 468
Kc/s Swedenr0ck080..Supermantv0
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked pass
ords reliably
Session completed.
h0n0pp1e@instance-1:~/JohnTheRipper/run$

```