📬 Submit this assignment by **Monday, March 13th at 11:59pm PDT** using the *Submit* button 👉

## **Project #3: Password Crack-a-thon**

### **Overview**

Warm up your skills with [John the Ripper](https://www.openwall.com/john/doc/), it's time for the CYB101 🔐 **crack-a-thon** 🔐.

For this project, you'll be working with a (fictional) **leaked password file**, modeled after famous data breaches such as the [2012 LinkedIn Hack](https://en.wikipedia.org/wiki/2012_LinkedIn_hack) and [2016 Yahoo Data Breaches](https://en.wikipedia.org/wiki/Yahoo!_data_breaches). In both of these incidents, usernames and hashed passwords were leaked in simple txt files, making people's private data available to anyone who could crack the hashes.

Your task is simple: Crack as many hashes as possible, so those passwords can be removed from production and those users' accounts secured.

### **🎯 Goals**

By the end of this assignment you will be able to...

* Write your own john commands to...
  + use multiple different wordlists
  + use built-in john rulesets
  + use custom-made rules
* Communicate your findings using the john.pot file

For this assignment, you'll be filling and submitting a copy of the [📄 **Project 3 Submission Template** (Google Doc)](https://docs.google.com/document/d/11xZIhWxMo2IYu5FZqoHnLSASXSwghAnKP6SEvsJCeiI/copy)

* Before proceeding, we recommend you **open it up now** and read over the requirements in the document.
* It might be easier to "fill-as-you-go" than try to fill it all out after you complete the project.

Required Challenges

*To receive full credit, you must...*

* **Crack at least 250 passwords**
  + This is 25% of the 1000 password file.
  + To check how many passwords you've cracked, run: john --show CPLeak.txt
* **Write a john command using a different wordlist**
  + For your lab, you were provided lower.lst, which is a pretty short file.
  + You'll need to use a bigger, better wordlist to crack enough of these passwords!
* **Write a john command using a built-in ruleset**
  + This will be some line with --rules=.
  + For a full list of rules, try running: grep -E "^\[List.Rules" /etc/john/john.conf
    - Or look inside the /etc/john/john.conf file for lines starting with [List.Rules...
* **Write a john command using a custom mask**
  + This will be some line with --mask=.
  + For more info on John rules syntax, see [the John docs](https://www.openwall.com/john/doc/RULES.shtml)

Close Section

Stretch Challenges

*To receive bonus points, you can...*

* Crack at least 500 passwords (tricky)
* Crack at least 750 passwords (hard)
* Crack all 1000 passwords (impossible)

Close Section

#### **🧩 The Data Set**

The password leaks are available in [CPLeak.txt](https://courses.codepath.org/course_files/cyb101/project_3/CPLeak.txt)

* To get the file on your Kali box, follow the instructions used for downloading crackfiles.zip in Step 1 of this week's lab.

Cracking the passwords with no prior knowledge is the most realistic option. However, it's also realistic for password crackers to spend days and even weeks cracking! 😩

To keep your time reasonable, We'll provide some helpful **statistics** about the passwords. It's up to you to figure out how to use this information!

🔑 CPLeak.txt Statistics

* **Total Number of Username/Password Hashes**: 1000
* **Primary User Language**: English
* **Password Length Distribution**:

| **Length (# chars)** | **Count (# passwords)** |
| --- | --- |
| 1 | 2 |
| 2 | 13 |
| 3 | 87 |
| 4 | 284 |
| 5 | 487 |
| 6 | 107 |
| 7 | 18 |
| 8 | 2 |

Close Section

Stretch Goals

### **Stretch Goals**

The stretch goals for the crack-a-thon are simple... How many passwords can you crack?

#### **(Optional) Crack 50% of the passwords**

* Crack 50% of the passwords and get 1 bonus point!

#### **(Optional) Crack 75% of the passwords**

* Crack 75% of the passwords for ANOTHER bonus point! (Stacks with previous bonus)

#### **(Optional) Crack 100% of the passwords (Really, really hard)**

* If you manage to crack them all... you get ANOTHER bonus point, and bragging rights for life!

Close Section

📘 Resources

* [John the Ripper docs](https://www.openwall.com/john/doc/)
* [John Custom Rules Syntax](https://www.openwall.com/john/doc/RULES.shtml)

Close Section

💡 Hints

* How long should this assignment take?
  + Password cracking is a funky art in that the time taken can vary wildly depending on how precise your commands are. (*Sure, you CAN just try inputting EVERY possible 5-digit password, but that will take a long time...*)
  + If you're clever about your choice of inputs, it's possible to get the required 250 cracks in under 30 minutes.
    - So, if you run a command and the ETA is next week... you might need to rethink your strategy.
* Help! I don't know where to start!
  + Look at the 🔑 CPLeak.txt Statistics provided in *Project Requirements*. What seems like it might be low-hanging fruit you can crack quickly and get out of the way?
  + Hint: Smaller passwords are easier to crack than longer ones -- try for those first.
* Why isn't my --mask= string working?
  + Unfortunately, the --mask syntax doesn't perfectly match the docs. (For example, ?v for "vowels" won't work with --mask!)
  + Working with outdated/incomplete docs is a realistic part of cybersecurity work... try substituting other options until you find something that works for you.
    - Hint: To do a mask with vowels, we substituted in the [RegEx](https://en.wikipedia.org/wiki/Regular_expression) [aeiou] for ?v.

Close Section

### **📬 Submitting Your Project**

* [📄 **Project 3 Submission Template** (Google Doc)](https://docs.google.com/document/d/11xZIhWxMo2IYu5FZqoHnLSASXSwghAnKP6SEvsJCeiI/copy)

✔ Am I Ready to Submit?

Check if you're **ready to submit** with the following questions:

* Did you complete all of the **Required Challenges**?
* Did you copy and fill out the [**Project 3 Submission Template**](https://docs.google.com/document/d/11xZIhWxMo2IYu5FZqoHnLSASXSwghAnKP6SEvsJCeiI/copy)?
  + It is important that you follow the same layout as the template so that we can easily access your work.
  + Be sure to check off each feature that is implemented in the **"Submission Checklist"** section
* Are any required images/GIFs correctly displaying in your document?
* Did you set your document to ***"Anyone with the link can Edit"***?

If you answered **yes** to **all** of these questions, you are ready to submit!

Look for the **"Submit"** button at the top of this page.

Close Section

📣 **Late Submissions**

* We highly encourage you submit your project in any state (even if it is not done) by the deadline: **Monday, March 13th at 11:59pm PDT**.
* You can continue to work on your project with our **48-hour extension** in which your project will be graded once more once the extension deadline has passed.
* Don't forget to **resubmit through the course portal** with your **updated document link**!