John the Ripper

# BACKGROUND

John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms. It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker.

It can be run against various encrypted password formats including several crypt password hash types (DES, MD5, or Blowfish, Kerberos AFS, and Windows NT/2000/XP/2003 LM hash). Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others[[1]](#footnote-0).

# REQUIREMENTS

An instance of Linux (a virtualized Kali Linux is cool because it comes with the RockYou password library - which is much bigger than the one that comes with John the Ripper, but you can use any distribution; this class recommends Ubuntu).

If you do not have John the Ripper installed, you will have to get it:

| sudo apt updatesudo apt install john |
| --- |

NOTE: John the Ripper may not function properly on some recent versions of Linux; you can always use the [Google Cloud Shell](https://shell.cloud.google.com/?show=terminal) for this lab (John the Ripper works well there).

# PART I: Create an account in Linux

1. From the command line, you will need to create an account. This will be temporary (we’ll be deleting it at the end of this lab). Let’s make the account your first name and any last name you’d like. We’ll use the program useradd. But there are two issues with this. The first is that useradd is not in our path (that’s like saying useradd is an application on the computer, but it’s not in our list of programs we can run). The other issue is that even if it *was* in our path, we are not an administrator, and we wouldn’t be able to run it anyhow. So we have to prepend the useradd call with sudo, which means “super user do” and let us run programs not in our path (and also as an administrator!). In my case, I’m going to use “DaveyG” as the user account:

**sudo useradd -m DaveyG**

Note that the -m attribute will ensure that a home directory will also be created for the user.

1. Next, let’s get DaveyG set up with a password. Since the dictionary that John the Ripper will be using is not sufficiently large, a simple password should be used here (since we’re trying to crack it). You *could* use rockyou.txt as the library (recall that it comes standard with Kali), but the default dictionary with John the Ripper is good enough for this exercise. If you want to use rockyou.txt with John the Ripper, [check out this article](http://www.solutionsatexperts.com/password-cracking-with-john-the-ripper-on-linux/).

**sudo passwd DaveyG**

You’ll enter the password twice (note that there may not be visual confirmation that you are entering a password until you press ENTER).

*Note that if you use a somewhat sophisticated password, John the Ripper won’t be able to crack the password you choose and you’ll need to choose an easier password to crack and do this again.* That isn’t to say that John the Ripper can’t crack more complex passwords (because it can); it’s just that the default wordlist that comes with John the Ripper is intentionally small. Passwords like 12345 and password are appropriate.

| EVIDENCE #1 |
| --- |
| **PASTE THE IMAGE OF CREATING THE ACCOUNT** |

# PART II: View the user accounts and their hashed passwords

1. It is important to know that in Linux, there is a file /etc/passwd that stores all the basic information about each user. This is normal for many operating systems, and you can view it with the cat command:

**sudo cat /etc/passwd**

1. It is also important to know that in Linux there is a file /etc/shadow that stores the hashed versions of user passwords. You can view it by using cat to output the data:

**sudo cat /etc/shadow**

Naturally, you won’t be able to decipher much more than the usernames in this file.

1. Lastly, it is imperative to know that John the Ripper comes with unshadow. All unshadow does is stitch together the passwd file and shadow file so John the Ripper can use it.
2. Let’s marry those two files together with Unshadow and prep it for John the Ripper. We’ll run unshadow and store the results in a file that we’ll create on the fly called tempUserPW:

**sudo unshadow /etc/passwd /etc/shadow > tempUserPW**

Let’s take a look and see if everything seems to be working so far:

**cat tempUserPW**

| EVIDENCE #2 |
| --- |
| **PASTE THE IMAGE OF RUNNING UNSHADOW AND CAT*[NOTE THAT THIS SCREENSHOT IS MISSING QUITE A BIT OF INFORMATION -THE IMPORTANT PART IS THE LAST FEW LINES]*** |

#

# PART III: Crack the password

1. Time to fire up John the Ripper! When we run John the Ripper, we’ll have to give it both the wordlist we want to use and the file we made with unshadow. Again, we’ll be using the standard dictionary that comes with John the Ripper, not rockyou.txt. If you wanted to use rockyou.txt, you’d have to point to it in the wordlist parameter. And you totally should for funsies!

**sudo john -wordlist=/usr/share/john/password.lst --format=crypt tempUserPW**

Yeah! We just cracked the passwords (at least, the ones that were easy to crack with the default dictionary). The output looks daunting, but it’s not too bad to decipher.



1. Happily our output shouldn’t be too cumbersome because there are only a few accounts. But if there were a lot of accounts, we could clean up the output with the show parameter in John the Ripper:

**sudo john -show tempUserPW**

| EVIDENCE #3 |
| --- |
| **IMAGE SHOWING THE CRACK AND ‘SHOW’** |

#

# PART IV: Delete the account you made

1. We’re done with the temporary account, so you can delete it if you’d like.

**sudo userdel DaveyG**

We can also delete the file we used to hold the results from unshadow:

**sudo rm tempUserPW**

# CONCLUSION

That’s it! We just cracked a Linux user account with John the Ripper. There were a few things that made this possible, but the biggest enabler is when we created a relatively weak password. This is meant to show just how weak some passwords are. Be careful when you make passwords for various accounts!

As mentioned, you could use rockyou.txt for a much broader dictionary attack.

Jack the Ripper can be used for much more than Linux passwords; [read up on it here](https://bytesoverbombs.io/cracking-everything-with-john-the-ripper-d434f0f6dc1c).

# WALKTHROUGH

[](https://www.youtube.com/watch?v=LpNpIwj-_Aw)

[YouTube Link](https://www.youtube.com/watch?v=LpNpIwj-_Aw)

1. [John the Ripper [Wikipedia]](https://en.wikipedia.org/wiki/John_the_Ripper) [↑](#footnote-ref-0)