



Tool of the Week: John the Ripper

By:

Brandon Aperochoco & Arjun Sharma

What is John the Ripper?

- One of the most powerful password cracking tool on Kali Linux
 - Johnny (GUI version)
- Can crack: **`/etc/shadow`** & **`/etc/passwd`** files, Encrypted ZIP/RAR files, etc.

Background Info: How Linux Login Works?

- 1) User enters password
- 2) Password is hashed with salt value and compared with the encoded password
- 3) If they match, the user is given access to the system
- *Note: Linux uses a salt that is between 1-4096
- UserID, roles, permissions is stored in **/etc/passwd**
- Passwords are stored in **/etc/shadow**

/etc/passwd & /etc/shadow

- Passwords are encrypted using the crypt() command
 - **\$6\$salt\$encrypted** is the typical output
 - The number **\$6** represents the type of encryption it is using
 - **\$Salt** is a randomly-generated string and **\$encrypted** is the hashed password
- /etc/passwd is world readable and passwords were stored here initially, this is not safe!
- So these passwords are now stored in /etc/shadow; only readable by root

| ID | Method |
|----|---|
| 1 | MD5 |
| 2a | Blowfish (not in mainline glibc; added in some Linux distributions) |
| 5 | SHA-256 (since glibc 2.7) |
| 6 | SHA-512 (since glibc 2.7) |

```
user001:$6$zhk6vfcz$z5acf0IZYEddqQkbz63Cj/7dWTNu40dLs4a0ZEbwfczFxFwGIY1d.DI4HuWoEtKXgwJuoDRIUmIFTMX23LUhHA/:1007:1007::/home/user001:/bin/sh
user003:$6$btprLZ8e$15yl1sICoLhUow9TjglawNPTKdJM6BMQg3kc9200ckLGX0Ec2W0XD2acCVWehpp.8GhgmwydKy.RiVzvVwgrS1:1008:1008::/home/user003:/bin/sh
user006:$6$Dobi4kHb$9C0Kai1PG7VsfVvxYjx0UyuQXorQQYFT0TEtKzNDaLZ0xVbL.7dq96kfmDHI6SbZmRSGGW.WTSoyQp1qNKLn51:1009:1009::/home/user006:/bin/sh
```

Demo

- Let's do a simple example of the usage of John the Ripper

3 Modes for John the Ripper

- Single crack (Simple rule-based algorithm)
- Wordlist (Dictionary attacks)
- Incremental (Brute force)
- *Note: The Default mode of John uses all three from top to bottom

John the Ripper Mode: **single**

- Typically want to use this mode first when attempting to crack passwords
- This mode attempts to crack using login/account information as passwords
 - Creates different permutations of the login/account info for JTR to use to crack passwords
 - IE. John Smith → johnsmith, john-smith, smithj, JoHNSMiTH, john1
- Demo!

Demo Recap

- Single ruleset located in `/etc/john/john.conf` and start at around line 400
- Ruleset contains about 200 rules
 - After 20 rules 50% of single passwords are cracked
- Can add/edit rules

John the Ripper Mode: **wordlist**

- John the Ripper does a dictionary attack with a provided list of words
 - You can use the provided password list located in `/usr/share/john/password.lst`
 - List is composed of the top 3000ish passwords from multiple websites
 - OR you can use a customized list you made
 - Each password is also applied to each rule to provided by `[List.Rules:Wordlist]`
 - IE. `password` → `Password1`, `drowssaP`, etc.
 - You can even add your own rules in `/etc/john/john/conf`
 - IE `[List.Rules:Easy]`

John the Ripper Custom Rules

```
cAz"[0-9]"  
cAz"[0-9][0-9]"  
cAz"[£!$]"  
cAz"[0-9][£!$]"
```

c = Capitalize the first letter
Az = Append to end of string
Things in quotes are what is being appended

```
#Prepends one, two, and three numbers to a password
```

```
^[0-9]
```

```
^[0-9]^[0-9]
```

```
^[0-9]^[0-9]^[0-9]
```

Seem familiar? Almost like something we learned... (Regular Expressions)

Note: There are many ways to do the same rule

Demo!

John the Ripper Mode: **incremental**

- John the Ripper performs a brute force attack to attempt to crack passwords
- There are modes to speed up the process
 - Alpha (Letters only)
 - Digits (Digits only)
 - lanman (Alphanumeric and some special chars)
 - All (all chars)
- Customize your brute force with rules, similar to wordlist
- Demo!
- Note: CharCount parameter affects the number of characters incremental will use. Having CharCount less than 95 will cause John to favour simpler, longer passwords over shorter, more complex passwords; most of the time you would not want this. Typically the standard user makes short but complex passwords.

Defending against JTR

- Inform users to create strong passwords
 - 8-10 characters is usually a good length
 - Using upper and lower case chars
 - Using special digits and special chars
 - Don't be predictable! IE Password1 vs Pass1word
- Use the mailer command; emails users if their password has been cracked by JTR
 - mailer PASSWORD-FILE
- Use unafs command; warns users about their weak passwords
 - unafs DATABASE-FILE CELL-NAME
- Run John on yourself or on your company database!
- Add a wait timer in between attempts
- Make sure that root privileged accounts are not vulnerable, otherwise can see /etc/shadow and su into other accounts

References

- <https://tools.kali.org/password-attacks/john>
- <https://www.openwall.com/john/doc/OPTIONS.shtml>
- <https://www.openwall.com/john/doc/MODES.shtml>
- <https://www.openwall.com/john/doc/EXAMPLES.shtml>
- <http://www.admin-magazine.com/Articles/John-the-Ripper>
- <https://countuponsecurity.files.wordpress.com/2016/09/jtr-cheat-sheet.pdf>
- <https://www.openwall.com/john/doc/RULES.shtml>