Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Linux Password Cracking: Explain unshadow and john commands (john the ripper tool)

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. Can you tell me more about unshadow and john command line tools? How does it protect my server from crackers?

A. Both unshadow and john distributed with - John the Ripper security software or fast password cracker software. It is free and Open Source software. It runs on Windows, UNIX and Linux operating system. Use this tool to find out **weak users passwords on your own server**.

John cracking modes

John can work in the following modes:
[a] **Wordlist** : John will simply use a file with a list of words that will be checked against the passwords. See RULES for the format of wordlist files.

[b] **Single crack** : In this mode, john will try to crack the password using the login/GECOS information as passwords.

[c] **Incremental** : This is the most powerful mode. John will try any character combination to resolve the password. Details about these modes can be found in the MODES file in john’s documentation, including how to define your own cracking methods.

Install John the Ripper Password Cracking Tool

John the ripper is not installed by default. If you are using Debian / Ubuntu Linux, enter:

```
$ sudo apt-get install john
```

Note: RHEL, CentOS, Fedora, Redhat Linux user can grab john the ripper here [2]. Once downloaded use rpm command:

```
# rpm -ivh john*
```

How do I use John the ripper to check weak passwords / crack passwords?

First use the unshadow command to combines the /etc/passwd [3] and /etc/shadow [3] files so John can use them. You might need this since if you only used your shadow file, the GECOS information wouldn’t be used by the "single crack" mode, and also you wouldn’t be able to use the -shells option. On a normal system you’ll need to run unshadow as root to be able to read the shadow file. So login as root or use old good sudo / su command under Debian / Ubuntu Linux:

```
$ sudo /usr/sbin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db
```

RHEL / CentOS / Fedora Linux user type the following command:

```
# /usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db
```

To check weak password (crack password), enter the following command:

WARNING! These examples uses brute-force ~ CPU-time consuming password cracking techniques.

To use John, you just need to supply it a password file created using unshadow command along with desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental" password cracking methods.

```
$ john /tmp/crack.password.db
```

Output:

```
 john  /tmp/crack.password.db
Loaded 1 password (FreeBSD MD5 [32/32])
```

This procedure will take its own time. To see the cracked passwords, enter:

```
$ john -show /tmp/crack.password.db
```

```
test:123456:1002:1002:test,,,:/home/test:/bin/bash
didi:abc123:1003:1003::/home/didi:/usr/bin/rssh

2 passwords cracked, 1 left
```

Above output clearly indicates - user test has 123456 and didi has abc123 password.

Related:

- Linux check passwords against a dictionary attack [4]
- John the ripper examples text file [5] for more information.

Further readings:

- John the ripper project [6] home page
- Refer john and unshadow command man page
- John the ripper examples text file [5]
- John configuration file /etc/john/john.conf

  Rainbow table [7] - Rainbow Cracking uses differs from brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password drastically. See Ophcrack [8] Live CD.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/linux/**
[2] john the ripper here: **http://dag.wieers.com/rpm/packages/john/**
[3] /etc/passwd: **http://www.cyberciti.biz/faq/understanding-etcshadow-file/**
[4] Linux check passwords against a dictionary attack: **http://www.cyberciti.biz/tips/linux-check-passwords-against-a-dictionary-attack.html**
[5] John the ripper examples text file: **http://www.cyberciti.biz/faq/wp-content/uploads/2008/01/john-the-ripper-examples.txt**
[6] John the ripper project: **http://www.openwall.com/john/**
[7] Rainbow table: **http://en.wikipedia.org/wiki/Rainbow_table**
[8] Ophcrack: **http://theos.in/windows-server/crack-a-windows-xp-or-vista-password/**

Further readings: