Linux Password Cracking: Explain unshadow and john Commands (John the Ripper Tool)

last updated September 17, 2014 **in Linux, Security, UNIX**

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

Both unshadow and john commands are distributed with “John the Ripper security” software. It act as a fast password cracker software. It is a 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** or workstation powered by Unix-like systems.

John cracking modes

[donotprint][/donotprint] John the Ripper 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 johnâ€™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
```

RHEL, CentOS, Fedora, Redhat Linux user can grab john the ripper here. Once downloaded use the rpm command as follows to install the same:

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

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

First use the unshadow command to combines the /etc/passwd and /etc/shadow files so John can use them. You might need this since if you only used your shadow file, the GECOS information wouldnâ€™t be used by the “single crack” mode, and also you wouldnâ€™t be able to use the -shells option. On a normal system youâ€™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 that user test has 123456 and didi has abc123 password.

RELATED:

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

Further readings:

- John the ripper project home page.
- See john and unshadow command man pages.
- John the ripper examples text file
- John configuration file /etc/john/john.conf
- Rainbow table – 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 Live CD.

Posted by: Vivek Gite

The author is the creator of nixCraft and a seasoned sysadmin, DevOps engineer, and a trainer for the Linux operating system/Unix shell scripting. Get the **latest tutorials on SysAdmin, Linux/Unix and open source topics via RSS/XML feed** or weekly email newsletter.

---

blink4blog January 12, 2008 at 3:38 pm

It clearly shows that the more complex and non-dictionary words we use, the longer it takes for John to crack them.

Rules of thumb,

– never use the same password forever, change it on a periodic time.

– don't use personal information as password or any partial of that

– mix numbers, punctuations. symbols if possible

– never share password to others

– never use root account for normal usage

– keep system up to date always

---

nixCraft January 12, 2008 at 3:44 pm

One more addition, give shell access only if required.

Nilesh January 12, 2008 at 5:40 pm

And one more- Disable unwanted features for users.
Like- SSH.

Anil Waghmare February 5, 2008 at 4:37 am

its better to make **/tmp/crack.password.db** to **/root/crack.password.db**. isn't it?

> **Jin** July 22, 2016 at 6:03 am
>
> sure! Thumbs up!

---

kojo May 21, 2008 at 10:39 pm

nice short tutorial: just a question though:
whats the equivalent of this command in non redhat variant systems where unshadow does not exist?
sudo /usr/sbin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db

---

nixCraft May 21, 2008 at 11:05 pm

unshadow is part of the package. It should be at /usr/sbin or /usr/local/sbin

---

Anant Bhasu May 26, 2008 at 8:49 am

Always take care that you dont alter the file permissions for the /etc/shadow file, which by default is "-r———" read only for root(This is definetly true for CentOS and FC,am not sure about the rest). If the read permissions are set for the user for /etc/shadow, a non root user may be able to execute john to retrieve passwords for root as well as other users on that system. Overall this system can then be viable to remote attacks via pre installed back door user

accounts.

Ashwani March 30, 2009 at 3:19 pm

Well i can say its simply doesnt work on tough passwords it works only on simple text passwords i dont know y this package got so...much of popularity

Ajit June 4, 2009 at 11:09 am

a simple steap is linux passwd

smith July 13, 2009 at 3:16 pm

I have recentaly accured some passwods and am in need of a nother there are 3 computers that anr pertected by passwords I have 2 of them but the last one evades me for computer 2 the password is 036915307. for computer3 the password is036915364.
i need the passwoed for computer1 the pass words goes 0369152 I could not figure out the res if some one would help i would appreat it.
smith

> **bo** May 24, 2010 at 3:57 pm
>
> sounds like phone numbers in the tel-aviv (israel) area codes :)

kalidoss August 5, 2009 at 9:57 am

Hi, this is working to crack the week passwords only, I can't crack my root password; how to crack touch passwords. If anybody know the solution, please mail me.

kalidosstvr@yahoo.in

---

fotis December 25, 2009 at 11:41 pm

really helpfull. thanks

N0x February 16, 2010 at 5:45 pm

I don't think JTR is compatible with the new SHA512 encryption on most Linux distributions...

---

unp September 29, 2010 at 1:11 am

N0x ye be right:
~$ john /tmp/crack.password.db
No password hashes loaded

> **Baby** June 16, 2011 at 2:30 pm
>
> me too!!

ki6i September 26, 2012 at 10:20 am

That simply means that there is no password hashes in the file, which you try to search into

Try with those:
num:CR9.E1Q9XBCbs:0:1:Operator:/:/bin/csh
dra:CR.L.LLfgc/5Y:0:1:Operator:/:/bin/csh
sec:CR6Xdsh28cJFA:0:1:Operator:/:/bin/csh

> **SHAmon** October 24, 2012 at 9:59 pm
>
> I think John the Ripper community-enhanced version supports SHA but the regular release does not, perhaps the John Pro supports SHA too...

---

bqcot December 13, 2010 at 6:12 pm

nice for dumies.. I'll try :)

Ashwin Hegde January 11, 2011 at 1:38 pm

Nice Application;

---

sanjay kumar verma February 21, 2011 at 6:16 am

Hello
dear....

how to break password of root in Rhel 6.0
Thanks

fub May 7, 2011 at 4:04 pm

I hav a problm when making a copy:
cp /etc/passwd > passwd.1—>cp: opÃ©rande du fichier cible manquant aprÃ¨s `/etc/passwd'
Pour en savoir davantage, faites: Â« cp –help Â».
Can someone help me!thank

jizzle May 25, 2011 at 7:16 pm

hey jabronis, this will work on strong passwords. it has a brute force mode which checks all possible combinations, you just have to be patient :p

webuser July 1, 2011 at 6:37 am

EPIC FAIL in ubuntu 11.04

> **jenkinbr** December 4, 2011 at 5:31 am
>
> Did you try installing from source? I had the same issue with the ubuntu binaries.

saint moses August 22, 2011 at 6:54 am

hey anybody..
tell me how to crack the login password ini ubuntu.
i've to use the software for crack but still doesnt work..
tell me sooner .
dhanke well

wrongname August 30, 2011 at 10:59 am

hello sir,
I forgot my ubuntu password so please help me. here no service center.

JD December 14, 2011 at 7:21 pm

Just saved me a lot of time!

'Hats off to John the Ripper'!!!

Kataklysmos February 9, 2012 at 11:01 am

I had the same problem (Debian squeeze), too. So I uninstalled "john" and "john-data" via apt-get and compiled it by myself. Now it is running wonderful!

@VIVEK: Thank you for this short but detailed article.

Pindour February 24, 2012 at 9:12 am

Can you please help, I can not decrypt.
root:KPcKrCeGUgGeA:1201282644:0:0

Thanks

Saqib December 28, 2012 at 5:12 pm

Hi in linux there is security password are locked .i dont know the password what should i do

suresh April 6, 2013 at 7:21 am

Hi ,
I am getting the following error on My RHEL6.3 machine. Can anyone help me?

john /root/crack.password.db
fopen: $JOHN/dynamic.conf: No such file or directory

> **instantaphex** July 4, 2013 at 12:40 am
>
> I ran into the same problem on CentosOS 6. You have to comment out a line in /etc/john.conf.
>
> Change .include to #.include
>
> For me it was line 1435.

r3v August 21, 2013 at 4:20 pm

can i use awk command for sort /etc/passwd and /etc/shadow , maybe on

/etc/shadow too much password stored , like output : cat /etc/passwd | awk /root/ combine with cat /etc/shadow , then unshadow them

Vijay February 17, 2014 at 6:05 am

Hi Guys,
Hey I don't find any package called john kindly guide me am using Rhel-6.4 how do i crack the password.

Martin February 17, 2014 at 6:29 am

it is taking more than an hour to crack will it take so.

vegesoft September 9, 2016 at 4:06 pm

Tengo un HP-UX, e este servidor no hay el archivo /etc/shadow. He intentado trabajar solo con el /etc/passwd pero no lo he logrado. No tengo estos problemas con Linux. Por favor, su apoyo para poder avanzar con el HP-UX.

Still, have a question? Get help on our forum!

Tagged as: active password cracking tool, centos password cracking, crack, cracker software, debian password cracking, fedora password cracking, how to hack password, john the ripper, john the ripper password, linux password cracking, linux password hack, linux password recovery, linux password security, linux password tool, password cracker for linux, password cracking

tool, password details, passwords, rhel password cracking, security software, unix password cracking, Easy