

Martin Fahlgren
Internet Teknik
Studium Hisingen

Projektarbete

Lösenordsknäckning

med John the Ripper

Inlämnad av
Mariella Eriksson
Massiel Jimenez

Vad är John The Ripper?

Om ditt passwd-program av någon anledning inte tvingar användarna att ha lösenord som är svåra att gissa, så kan det vara lämpligt att köra ett program som försöker knäcka lösenorden för att försäkra dig om att användarnas lösenord är säkra.

John the Ripper är ett lösenordsknäckningsprogram skapat av Solar Designer. Den kan användas till UNIX, DOS och Win32.

Programmet kan endast utföra så kallade ordlisteattacker, den söker till att börja med i en ordlista, och fortsätter sedan själv att generera möjliga lösenord.

I Windows körs programmet från kommandotolken.

Man kan även knäcka Unixlösenord genom att komma åt shadow-filen.

Det finns en hel del växlar till programmet och är därför ganska svårt att lära sig helt och hållet, till skillnad från Tex lophtcrack.

Programmet skiljer inte på gemener och versaler.

Det finns en ordlista i programmet redan när man laddar ner det, men den är ganska dålig så det är bättre att hämta en mer omfattande ordlista på Internet.

Ordlistan sparas i /john-1.6/run-mappen.

Sedan skriver man in namnet på ordlistan i john-1.6/run/john.ini-filen.

Fördelar

John The Ripper är väldigt snabbt och det är gratis.

Du kan som administratör testa lösenorden på ditt nätverk för att få användare med dåliga lösenord att göra de säkrare. Observera att en inkräktare först måste hitta en säkerhetsläcka för att komma åt din shadow-fil (unix /etc/shadow), men dessa är vanligare än du kanske tror.

Nackdelar

Programmet använder mycket CPU-tid.

Ett problem med programmet är att man måste komma åt shadow filen för att kunna använda programmet, och man måste vara root för att genomföra lösenordsknäckningen.

Olika växlar som kan användas i programmet.

```

"\nJohn the Ripper  Version " JOHN_VERSION \
"  Copyright (c) 1996-98 by Solar Designer\n" \
"\n" \
"Usage: %s [OPTIONS] [PASSWORD-FILES]\n" \
"-single                \"single crack\" mode\n" \
"-wordfile:FILE -stdin  wordlist mode, read words from FILE or stdin\n" \
"-rules                 enable rules for wordlist mode\n" \
"-incremental[:MODE]   incremental mode [using section MODE]\n" \
"-external:MODE        external mode or word filter\n" \
"-stdout[:LENGTH]     no cracking, just write words to stdout\n" \
"-restore[:FILE]      restore an interrupted session [from FILE]\n" \
"-session:FILE         set session file name to FILE\n" \
"-status[:FILE]       print status of a session [from FILE]\n" \
"-makechars:FILE      make a charset, FILE will be overwritten\n" \
"-show                 show cracked passwords\n" \
"-test                 perform a benchmark\n" \
"-users:[-]LOGIN|UID[,..] load this (these) user(s) only\n" \
"-groups:[-]GID[,..]   load users of this (these) group(s) only\n" \
"-shells:[-]SHELL[,..] load users with this (these) shell(s) only\n" \
"-salts:[-]COUNT     load salts with at least COUNT passwords only\n" \
"-format:NAME          force ciphertext format NAME " \
" (DES/BSDI/MD5/BF/AFS/LM)\n" \
"-savemem:LEVEL       enable memory saving, at LEVEL 1..3\n"

```

Installation/test

Först hämtar man hem programmet, packar upp det och lägger det i sin hemmapp:

Sedan går man in i john-1.6/src- mappen och gör filen körbar:
make linux-x86-any-elf

Efter det går man in i john-1,6/run-mappen

Där kör jag programmet:
./john /etc/shadow

Nu söker den igenom hela ordlistan.

Vi har laddat hem olika ordlistor från nätet som vi testar för att se om dom kan knäcka vårt lösenord:

Actor-givenname.lst
./john /etc/shadow

```
linux:/home/marielle/john-1.6/run # ./john /etc/shadow
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/32])
guesses: 0 time: 0:00:00:04 0% (2) c/s: 1514 trying: Arik
guesses: 0 time: 0:00:00:05 0% (2) c/s: 1516 trying: Choosri
guesses: 0 time: 0:00:00:06 0% (2) c/s: 1510 trying: Eisi
guesses: 0 time: 0:00:00:07 0% (2) c/s: 1514 trying: Grady
guesses: 0 time: 0:00:00:42 9% (2) c/s: 1503 trying: Dita1
guesses: 0 time: 0:00:00:44 9% (2) c/s: 1505 trying: Jigue11
guesses: 0 time: 0:00:00:45 9% (2) c/s: 1505 trying: Lucero1
█
```

common-passwords.lst:
./john /etc/shadow

```
linux:/home/marielle/john-1.6/run # ./john /etc/shadow
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/32])
guesses: 0 time: 0:00:00:04 0% (2) c/s: 1468 trying: irene
guesses: 0 time: 0:00:00:05 4% (2) c/s: 1478 trying: Ginger
guesses: 0 time: 0:00:00:06 5% (2) c/s: 1488 trying: erenities
guesses: 0 time: 0:00:00:07 7% (2) c/s: 1495 trying: dial1
guesses: 0 time: 0:00:00:08 9% (2) c/s: 1500 trying: Code1
guesses: 0 time: 0:00:00:09 10% (2) c/s: 1498 trying: castlecastle
guesses: 0 time: 0:00:00:11 14% (2) c/s: 1507 trying: lhutchins
guesses: 0 time: 0:00:00:17 24% (2) c/s: 1515 trying: ann9
guesses: 0 time: 0:00:00:18 26% (2) c/s: 1516 trying: xyzyy9
guesses: 0 time: 0:00:00:19 27% (2) c/s: 1516 trying: tuttle5
guesses: 0 time: 0:00:00:20 29% (2) c/s: 1518 trying: suzie4
guesses: 0 time: 0:00:00:21 31% (2) c/s: 1516 trying: saxon8
guesses: 0 time: 0:00:00:22 32% (2) c/s: 1517 trying: qwerty6
guesses: 0 time: 0:00:00:23 34% (2) c/s: 1518 trying: patty0
guesses: 0 time: 0:00:00:24 36% (2) c/s: 1518 trying: morley.
guesses: 0 time: 0:00:00:25 37% (2) c/s: 1518 trying: lock?
guesses: 0 time: 0:00:00:26 41% (2) c/s: 1519 trying: spprt
█
```

ASSurnames.lst:
./john /etc/shadow

```
linux:/home/marielle/john-1.6/run # ./john /etc/shadow
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/321])
guesses: 0 time: 0:00:00:17 (3) c/s: 1403 trying: batie1
guesses: 0 time: 0:00:00:20 (3) c/s: 1393 trying: megend
guesses: 0 time: 0:00:00:21 (3) c/s: 1393 trying: bugar
guesses: 0 time: 0:00:00:22 (3) c/s: 1394 trying: samaris
guesses: 0 time: 0:00:00:56 (3) c/s: 1446 trying: salmh1
guesses: 0 time: 0:00:00:57 (3) c/s: 1446 trying: dudo
guesses: 0 time: 0:00:00:58 (3) c/s: 1446 trying: apo
guesses: 0 time: 0:00:00:59 (3) c/s: 1446 trying: mike156
guesses: 0 time: 0:00:01:01 (3) c/s: 1443 trying: clasha
guesses: 0 time: 0:00:01:02 (3) c/s: 1444 trying: canart
guesses: 0 time: 0:00:01:03 (3) c/s: 1445 trying: clast1
guesses: 0 time: 0:00:01:04 (3) c/s: 1446 trying: calle1
guesses: 0 time: 0:00:01:05 (3) c/s: 1443 trying: shician
guesses: 0 time: 0:00:01:06 (3) c/s: 1441 trying: shilbee
guesses: 0 time: 0:00:01:07 (3) c/s: 1438 trying: mulie
guesses: 0 time: 0:00:01:08 (3) c/s: 1436 trying: bakio
guesses: 0 time: 0:00:01:09 (3) c/s: 1435 trying: metio
guesses: 0 time: 0:00:01:10 (3) c/s: 1433 trying: m1966
guesses: 0 time: 0:00:01:11 (3) c/s: 1430 trying: 14295
guesses: 0 time: 0:00:01:12 (3) c/s: 1428 trying: cocmi
guesses: 0 time: 0:00:01:13 (3) c/s: 1425 trying: sathead
```

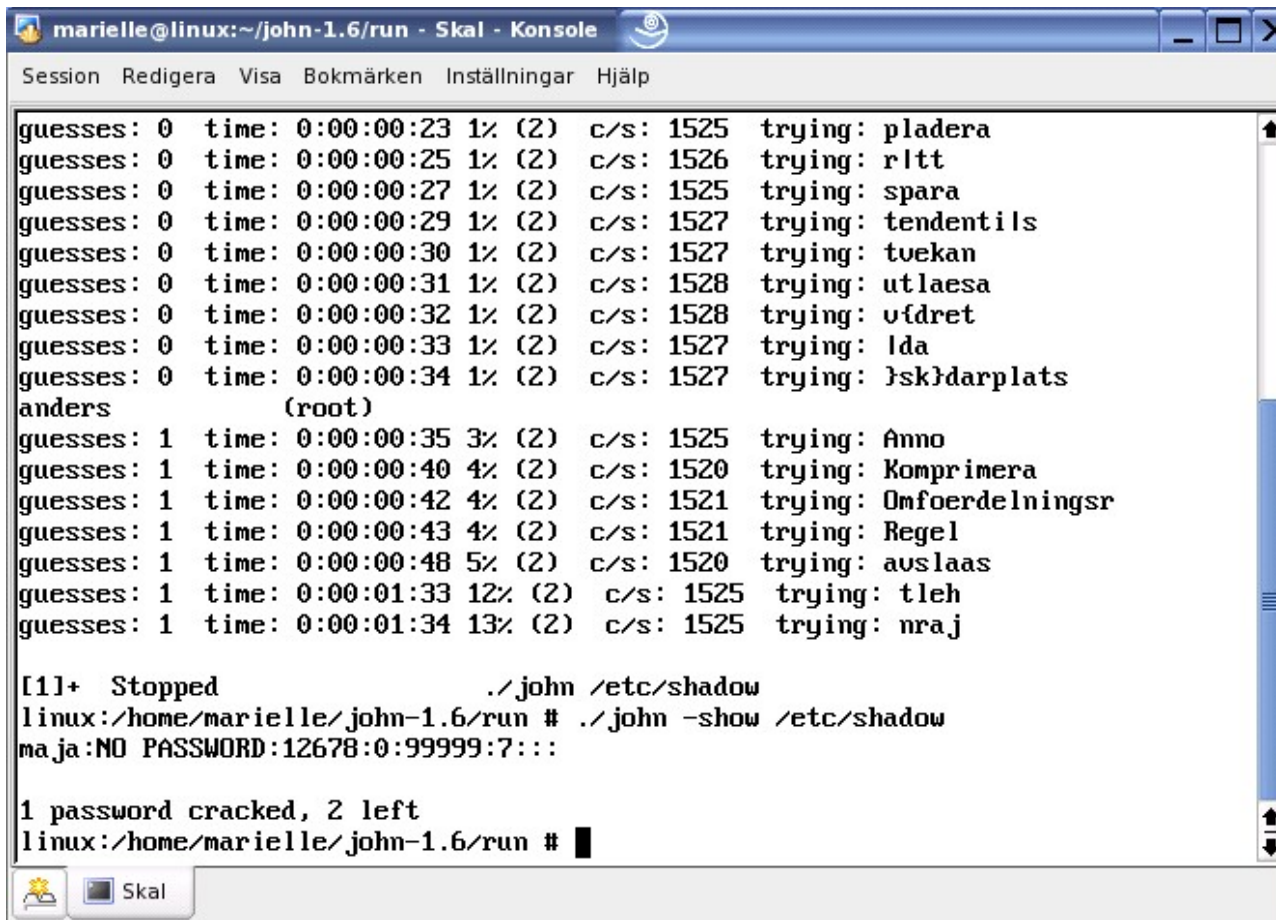


Vi testade även ordlistor med svenska ord.
Swedish.words.lst

```
linux:/home/marielle/john-1.6/run # ./john /etc/shadow
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/321])
guesses: 0 time: 0:00:00:03 83% (1) c/s: 1408 trying: Root58
guesses: 0 time: 0:00:00:05 0% (2) c/s: 1429 trying: anmflan
guesses: 0 time: 0:00:00:07 0% (2) c/s: 1424 trying: besllt
guesses: 0 time: 0:00:00:08 0% (2) c/s: 1436 trying: buske
guesses: 0 time: 0:00:00:10 0% (2) c/s: 1428 trying: erfarenhet
guesses: 0 time: 0:00:00:11 0% (2) c/s: 1436 trying: formler
guesses: 0 time: 0:00:00:13 0% (2) c/s: 1434 trying: generellt
```



Här har programmet knäckt root-lösenordet:



```
marielle@linux:~/john-1.6/run - Skal - Konsole
Session Redigera Visa Bokmärken Inställningar Hjälp
guesses: 0 time: 0:00:00:23 1% (2) c/s: 1525 trying: pladera
guesses: 0 time: 0:00:00:25 1% (2) c/s: 1526 trying: rltt
guesses: 0 time: 0:00:00:27 1% (2) c/s: 1525 trying: spara
guesses: 0 time: 0:00:00:29 1% (2) c/s: 1527 trying: tendentils
guesses: 0 time: 0:00:00:30 1% (2) c/s: 1527 trying: tuekan
guesses: 0 time: 0:00:00:31 1% (2) c/s: 1528 trying: utlaesa
guesses: 0 time: 0:00:00:32 1% (2) c/s: 1528 trying: v{dret
guesses: 0 time: 0:00:00:33 1% (2) c/s: 1527 trying: lda
guesses: 0 time: 0:00:00:34 1% (2) c/s: 1527 trying: }sk}darplats
anders
(root)
guesses: 1 time: 0:00:00:35 3% (2) c/s: 1525 trying: Anno
guesses: 1 time: 0:00:00:40 4% (2) c/s: 1520 trying: Komprimera
guesses: 1 time: 0:00:00:42 4% (2) c/s: 1521 trying: Omfoerdelningsr
guesses: 1 time: 0:00:00:43 4% (2) c/s: 1521 trying: Regel
guesses: 1 time: 0:00:00:48 5% (2) c/s: 1520 trying: avslas
guesses: 1 time: 0:00:01:33 12% (2) c/s: 1525 trying: tleh
guesses: 1 time: 0:00:01:34 13% (2) c/s: 1525 trying: nraj

[1]+ Stopped ./john /etc/shadow
linux:/home/marielle/john-1.6/run # ./john -show /etc/shadow
maja:NO PASSWORD:12678:0:99999:7:::

1 password cracked, 2 left
linux:/home/marielle/john-1.6/run # █
```