John the Ripper (ili kako odabrati dobru zaporku)

Provala na računalne sustave je bilo i bit će. Efikasnog recepta kako ovo spriječiti "jednom za svagda" nema, no problem se može ublažiti konstantnim obrazovanjem kako sistem-inženjera, tako i krajnjih korisnika. Naravno da korisnike nije prihvatljivo učiti o kriptografskim metodama i *one-time* zaporkama, ali ih možemo podučiti kako odabrati dobru zaporku. Ni u kojem slučaju zaporka ne smije biti iz rječnika, bilo engleskog, bilo kojeg drugog jezika. Zaporke koje su poznati pojmovi iz okolice korisnika, imena bliže rodbine ili kućnih ljubimaca su jako podložne socijalnom inženjeringu i ne treba ih rabiti. Zapravo,
najbolje je rabiti nekakav generator slučajnih zaporku, poput pwgena [1]. No, korisnici možda ne žele ili ne mogu zapamtiti ovakve zaporke i opet imamo problem.

Kad nemamo kontrolu nad zaporkama korisnika, ili smo naslijedili sustav pa ne znamo koliko su zaporke korisnika "snažne", jedino što možemo pokušati je poslužiti se alatima koji pokušavaju probiti zaporke korisnika, rabeći pri tome
različite tehnike. Nećemo previše ulaziti u te *password cracking* tehnike, spomenut ćemo samo rječničke napade (kada se rabe riječi iz različitih rječnika ili jednostavno zbirki riječi), te *brute-force* napade (kad se pokušava probiti zaporku nizanjem znakova po redu, "aaaa", "aaab", "aaac" itd).

No, dosta često se s nekog udaljenog (napadačkog) računala pokušavaju probiti korisnički računi, tako da se nižu već negdje snimljene zaporke. Obično se napdaju neki od poznatih serivsa, kao što su ftp, ssh ili SASL. Isto tako, razni trojanski programi na PC računalima znaju presresti korisničke zaporke i poslati ih na direktno napadaču. Sve to rezultira slanjem spama preko vašeg vlastitog poslužitelja, u zadnje vrijeme najčešće SASL servisa, koji je po *defaultu* uključen u CARNetovu distribuciju Debiana.

Podsjetimo se, SASL omogućava korisnicima da pošalju mail s bilo koje adresu na Internetu rabeći svoju zaporku, i na taj način zaobilazi "*relay denied*" poruke.

Ipak, dosta često je riječ o slabim zaporkama, pa nam ostaje zadatak kako ih pronaći. Upotrijebit ćemo jedan od češćih programa za *cracking* zaporki, John the Ripper. Instalacija je jednostavna:

```
# apt-get install john
...
Setting up john-data (1.7.2-3) ...
Setting up john (1.7.2-3) ...
mode of /var/run/john' changed to 0700 (rwx------)
#
```

Prvo što ćemo napraviti je spojiti /etc/shadow i /etc/passwd datoteku u jednu. Za to postoji alat "unshadow":

```
# unshadow /etc/passwd /etc/shadow > zaporke.txt
# tail -5 zaporke.txt
idamjan:$1$T7sE9f3t$Re35DjBvrXejhrC.IyBtg1:2411:2411:Irena Damjan:/home/idamjan:/bin/
sh
jperic:$1$t7qUAsJa$o.RUrOWABsfdjdQRE.nHE.:2412:2412:Julijana Peric:/home/jperic:/bin/
sh
```

```
jgadzo:$1$8hXNr3DD$dfghhheagdyrJwKOVS7jr/:2413:2413:Jelena Gadzovic:/home/jgadzo:/bin
/sh
mpehar:$1$wr4So1k6$Xzc;lkjdsokfsJHY.tLAU/:2414:2414:Mirta Peharcic:/home/mpehar:/bin/
sh
gjurkovi:$1$9UwQK8M5$ZrQ4hHKJK6khjduDXagIX/:2415:2415:Goran Jurkovic:/home/gjurkovi:/
bin/sh
```

Ova novonastala datoteka sadrži i zaporke i korisnička imena, pa je stoga bitno da je zaštitite od čitanja bilo kome osim korisniku root.

```
# chown root:root zaporke.txt
# chmod 600 zaporke.txt
```

Obećali smo da nećemo ulaziti previše u detalje, jer tražimo samo slabe zaporke pa nam naprednija podešavanja ni ne trebaju. U tome će nam pomoći i sam John the Ripper, koji, ukoliko ne navedete nijednu opciju, automatski rabi 3 najbitnija načina *crackiranja* zaporki: *single* način (pokušava pogoditi zaporku samo na osnovu podataka iz GECOS polja), rječnički napad (pokušava pogoditi zaporku na osnovu riječi iz rječničkih datoteka) i inkrementalni način (*brute force* napad s kombinacijama bilo kojih znakova, a sama duljina nizova se s vremenom povećava).

Da vidimo kako to izgleda:

```
# john zaporke.txt
Loaded 181 password hashes with 181 different salts (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:00:13 7% (1)  c/s: 7693  trying: madjericmarina7
guesses: 0  time: 0:00:00:15 8% (1)  c/s: 7709  trying: mandagaspard
guesses: 0  time: 0:00:00:16 8% (1)  c/s: 7729  trying: nikolzh
guesses: 0  time: 0:00:00:18 9% (1)  c/s: 7764  trying: mbmatagurn
guesses: 0  time: 0:00:00:19 10% (1)  c/s: 7755  trying: josipf
guesses: 0  time: 0:00:00:20 10% (1)  c/s: 7769  trying: sikicw
guesses: 0  time: 0:00:00:22 11% (1)  c/s: 7771  trying: nmatanicnina%
```

Svaki put kada stisnete tipku <enter>, ispisat će se statistika, te koja se zaporka trenutno pokušava pogoditi. Iz ovoga se jasno vidi na koji način john radi: dodaje razne dodatne znakove, uključujući i interpunkcije, pokušavajući emulirati način na koji korisnici biraju zaporku i tako ubrzati proces pronalaženja zaporke (ovo radi u bilo kojem načinu rada, *single*, *dictionary*...).

Iako se otkrivene zaporke prikazuju na ekranu, i naknadno možete vidjeti pogođene zaporke rabeći opciju "-show":

```
# john -show zaporke.txt
```

Iz ovoga je sasvim jasno da zaporke tipa "test123" ili "korisnik222" ne mogu biti dobre. Ovakve, ali i kompleksnije permutacije dolaze i s drugim načinima rada, stoga se za dobru zaporku, ponavljamo, obratite specijaliziranim programima.

Umjesto toga, možete upotrijebiti i jedan stari trik: uzmite neku rečenicu koju znate napamet (npr. poslovica), te odaberite samo prva slova. Primjerice:

`Bolje vrabac u ruci, nego golub na grani.` -> **Bvurngng**

Ovakve zaporke nema u nijednm rječniku, a *brute force* metodom će trebati previše vremena da se

zaporka pronađe. No, vi ćete ovakvu zaporku moći lakše zapamtiti nego nekakav slučajni niz znakova. Također, ukoliko stavite pokoji interpunkcijski znak ili veliko slovo, dobit ćete dosta sigurniju zaporku, primjerice:

`BvuR,ngNG!`

O ovoj temi se mogu napisati stranice i stranice teksta, ali vas nećemo previše zamarati s kriptografskim temama (osim ako sami ne pokažete zanimanje!). Vrijedi zapamtiti samo to da nikada nećete imati siguran sustav dok su korisničke zaporke slabe. Pomoću sigurnosne politike i u suradnji s upravom vaše institucije, naučite korisnike kako odabrati dobru zaporku. Svakako povremeno "provrtite" John the Ripper (primjerice preko noći) i provjerite ima li kakvih problematičnih zaporki na sustavu.

Sretno!

- Logirajte [2] se za dodavanje komentara

pon, 2011-01-31 22:08 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Software [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr./node/816

Links
[1] https://sysportal.carnet.hr./node/745
[2] https://sysportal.carnet.hr./sysportallogin
[3] https://sysportal.carnet.hr./taxonomy/term/17
[4] https://sysportal.carnet.hr./taxonomy/term/25