

Tek-Kullanımlık Şifreler

Uzunveözlüktebulunmayacak,sayıvekarakterlerdenoluşanenaz8haneli şifre kullanımtabiki güvenliğini artırarak, şifre güvenliğini artırarak şifreler seçmekten başka bir yöntem yokmu? İşte bu yazıda bu konuyu tartışacağız.

Normalde FreeBSD sisteminize girdiğinizde size kullanıcı adınız ve şifrenizi sorulur. Bu tür şifrelere, sisteme her girdiğinizde aynı şifreyi kullanıyorsunuz. Bu şifreyi değiştirebileceğiniz için, "Tekrar kullanılabilir şifre" adını veriyoruz. Bu da tabiki güvenlik olarak şifrenizi bilmeyen kimsenin sisteminize girmeyeceğini varsayar. Belgelerinizi de şifreli olarak saklayabilirsiniz. Sisteminizde bulunan başka kullanıcılarınızın şifrenizi bulması ise butun bir yöntem sonunu getirmekte.

Sistem güvenliğini için bunun yanında kullanılabilecek bir yöntem ise OTP (Tek kullanımlık şifreler). İsminden de anlaşılacağı gibi, tek şifreyi sadece bir kere kullanabiliyor ve aynı şifreyi birdah kullanamıyorsunuz. Böylece başka kullanıcıların şifrenizi öğrenemeyeceğini varsayar. Güvenlik açısından şifre kırıcılar, paket yakalayıcılar ve keylogger şeklinde adlandırılan yazılımların şifrelerinizi okuyabildiği varsayılır. OTP sisteminin hakkındaki RFC' lere İnternet sayfasından ulaşabilirsiniz.

OTP` ye giriş

OTP şu anda Telcordia olarak adlandırılan Bellcore` da S/Key adıyla anılan ve başta bedava olarak dağıtılan bir program olarak geliştirilmişti. Eğer bu konuda daha fazla bilgi almak isterseniz hakkındaki yazıyı ² adresinden okuyabilirsiniz.

Bellcore daha sonra S/Key isimli bir yayıncıyı kullanarak geliştirmeye başladı. Yazılım başka bir yerde OPIE (Her şeyde tek kullanımlık şifre) adıyla devam etti. Daha sonra ise OTP donanımlarında kullanılan hale geldi. Yazılım ve donanım olarak geliştirmenin detaylı şekli de bu ³ sayfadan okuyabilirsiniz.

Benim gibisi zinde FreeBSD sisteminize OTP` yi donanımlar olarak ekleyebilmek için gerekli parçaları alabileceğiniz kadar zengin olmadığımızı varsayıp sadece yazılımları eklemeyi göstereceğim.

OTP FreeBSD sisteminize beraber gelmekte. Eğer FreeBSD 4.x veya daha önceki versiyonun kullanıyorsanız muhtemelen hem `/usr/local/etc/skey` hem de `/usr/local/etc/opie` sisteminizde yüklüdür. Bunlardan `/usr/local/etc/opie` MD5 kullanırken `/usr/local/etc/skey` MD4 kullanmakta. Buyuzden FreeBSD 5.0` dan itibaren artık `/usr/local/etc/skey` yerini `/usr/local/etc/opie` ye bırakmakta. Buyuzden `/usr/local/etc/opie` nin konfigürasyonunu görecekmişiz.

OTP`nın Başlatılması

Opie`yi kullanmaya başlamadan önce kendinizi `/etc/ophiekeys` altındaki bulunan veritabanına eklemeniz gerekiyor. Bunun için `opiepasswd` komutunu kullanacağız:

```
$ opiepasswd -c
Adding dlavigne6:
Only use this method from the console; NEVER from remote. If you are
using
telnet, xterm, or a dial-in, type ^C now or exit with no password.
Then run opiepasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Secret pass phrases must be between 10 and 127 characters long.
Enter new secret pass phrase:
Again new secret pass phrase:

ID dlavigne6 OTP key is 499 dh0391
CHUG ROSA HIRE MALT DEBT EBEN
```

Bu komutu çalı ştırdığımda neler oldu ğunayakından bakalım. `opiepasswd -c` komutunu ancak sistemimizin başında yazılsel olarak otururken veya `ssh` ile başlıken kullanmalısınız. Eğer buna uymaz ve örne ğintelnet ile başlıken bu komutu kullanırsanız kullanacağınız şifre ve bunun sonucunda oluş turulacak tek kullanımlık anahtara ğ üzerinden açılarak gönderilecek ve a ğımızı dinleyen herhangi birisi bu şifreyi alıp OTP kullanmanıza ğmen hesabınızı kullanabilecektir.

Bu işlem den sonra, şifrenin çok kısa oldu ğuna dair bir uyarı ile birlikte, ikinci kez şifre girmem istendi. Olu şturulan bu şifre aynı şş şifreleme yönteminde kullanılan anahtar ile aynı şekilde çalı şmakta. Bu her kullanıma açılışındaki kullanılacak aynı şifre olarak de ğil, benim veritabanına `dlavigne6` hesabını ekleyenki ş oldu ğum ve sonucunda tek kullanımlık şifrenin sahibi oldu ğumugösterir anahtar olarak kullanılmaktadır.

Bu noktada `opie` veritabanında oldu ğumudo ğrulayabilirim:

```
$ more /etc/ophiekeys
dlavigne6 0499 dh0391                669a4a62db6714f3  Jan 18, 2003 15:25:44
```

Bu çıktı da ğörebilece ğiniz gibi isim teksatırda; bir sayı (499), bir kod (dh0391) ile bunuzu izleyen anahtar (669a4a62db6714f3) ve tarihten oluş turulmuş olu şmakta. Burada kullanılacak sayı ve kod her şifre yaratılışındaki kullanılacak ğından önemlidirler.

Kod ve sayı de ğerlerinizi şu şekilde kontrol edebilirsiniz:

```
$ opieinfo
498 dh0391
```

`opieinfo` komutu sistem bir sonraki giri şimde kullanılacak olan sayı ve kodun sayısını göstermektedir. Burada giri ş numarası "498" ile ilgili şkilendirilmiş kodun bekledi ğine dikkat

edin. Ben sadece "499" ile ilgili şifrelenmiş kod bulmaktayım. Bir sonraki girişte kullanılacak kod bulabilmek için bir hesaplayıcı kullanmam gerekecek, burada ise hesaplamayı üstlenen program `opiekey` komutu olmaktadır.

Sisteme giriş

Bu noktada iki seçeneğim var: Ya her terminal girişi için de başka bir terminal üzerinde `opiekey` komutunu kullanarak veri girmek istediğim terminali yazarmıyım ya da kendime bütün kodların çıktısını alırsam bunları bittiriyenlerini yazdırırım. Her ikisini de deneyelim:

```
login: dlavigne6
otp-md5 498 dh0391 ext
Password:
```

Sistem girişimde OTP sistemi ben karışılıyor. `opie498` numarası ile ilgili şifrelenmiş tek kullanımlık şifreyi beklemekte. Normalde kullanıcıların sistem girişlerinde OTP kullanıp kullanmamak arasında seçimi yapabilmemiz gibi bir şans bulunmamaktadır. Bu yüzden her zaman kullanılmayan şifremi girersem yine kabul edilip sisteme girebilirim.

Eğer OTP kullanarak giriş yapmak istersem gerekli olan anahtar hesaplamam gerekmekte. Nerde hesapladığımız, şifrelenmemiş bir başlangıçta kullanılmadan sonra fark etmiyor. Bunun için Alt-F3 kullanarak diğer terminali geçip oradan hesaplayıcıyı çalıştırabilirim. Hesaplayıcıyı kullanabilmek için üç şey bilmem gerekiyor:

- kullanılacak sayı
- sayı numarası ile ilgili şifrelenmiş kod
- şifre

Burada önem verilmesi gereken şey her zaman gibi şifrenin bilinmemesidir. Şifre bilene kadar şifre sadece ben tek kullanımlık şifreyi üretebilirim sisteme girebilirim.

`Opiekey` komutunu kullanırken, giriş yaparken şifre sayacının numarasını da giriyorum:

```
$ opiekey 498 dh0391
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
MASK BALM COL HER RIFT TERM
```

İşlem sırasında şifreminde sorulduğundan itibaren. Bunun sonucunda 498 sayacıyla ilişkilenilen şifre: MASK BALM COL HER RIFT TERM olarak gözükte.

Şimdiartıkdogru şifreyibildigimegöregeridönüpdı ğerterminaldengirebilirim:

```
login: dlavigne6
otp-md5 498 dh0391 ext
Password: (here I pressed enter)
otp-md5 498 dh0391 ext
Password [echo on]: mask balm col her rift term
```

Buseferisetekrarkullanılabilir şifremigirmekyerine,Entertu şunabasıpecho`yu açıyorum.Tekrarkullanılabilinen şifreleringirilmesisırındaherzamankapalıolan bu özellikbençiktıolarakaldı ğım şifreyigirerkenbirisibenigörsebileayni şifreyi kullanarakistemegiremeyece ği içinOTPkullanımısırındaaçıkkalabiliyor.Ayr ıca tekrarkullanılabilir şifrelerinaksinebüyük/küçükharfayırımıönemliol muyor.

Şuandae ğer opieinfo komutunuverirsem497sayacıylakullanılacak şifreyi görebilirim.Farkedebileceginizgibihertekkullan ımlık şifrekullanılı şındasayaçbir azalmaktabuyüzden0ayakla ştı ğımdayenianahtarlarolu şturmamgerekecek.

Çoklu Anahtar Üretimi

Hergiri şyapmayaçalı ştı ğınızdayenibiranahtarüretmeksıkıcıbirdurumha lini alabilir.Buyüzdentümkodlarilistelememizeizinv erenikincigiri şyolumuzagözatalım.

Busefer opiekey komutuilekaçtanekodüretmekistedi ğimegörebirnumaraveya n parametresinikullanaca ğım.Örneğin497ileba şlayanbundansonraki10kodunçıktısını almayıdeneyelim:

```
$ opiekey -n 10 497 dh0391
```

```
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
488: COIN LO DOG GOLF ACTA FULL
489: SOD STUN SINK DRAW LAWN TILT
490: MALT STAY MASH CAR DEBT WAST
491: HOWE DRY WALL TOO BUDD SWIM
492: ROOT SPY BOND JEST HAIL SCAR
493: MEAN ADD NEON CAIN LION LAUD
494: LYLE HOLD HIGH HOME ITEM MEL
495: WICK BALI MAY EGO INK TOOK
496: RENT ARM WARN ARC LICE DOME
497: LEAD JAG MUCH MADE NONE WRIT
```

Bundansonrakullanaca ğım10 şifreyibildi ğimegöreartık bunlarıyabirka ğıdayazıp cüzdanımakoyabilirveyakomutsonucundaaldı ğımçıktıyı sistemüzerindebirdosya olarak yazabilirim.çıktıyıba şkabirdosyaolarakkullanmak için şukomutukullanabilir:

```
$ opiekey -n 10 497 dh0391 > secretlist
```

vedahasonrayazıcıdançiktısınıalabilirim.çiktısınıaldıktanonsistemimizdekibu dosyayısildi ğinizdeneminolun.Zirae ğersistemde bırakırsanızgüvenlikaçısından yaptığınızbunca şeybo şagidebilir.

Eğersayacımartıksonlarageldiysetekraryeni şifrelerüretmemgerekecektir.Bunuda opiepasswdkomutuyalayabilirim. Şifreveritabanındaoldu ğumiçinartık cparametresi yerine nparametresinive sparametresiniberaberkullanabilirim.Sayacı499` a ayarlayıpkodumudh1357olarakbelirlemekiçinsua ndakullandı ğimiçingeçerliolan kodugirmemgerekecek:

```
$ opiepasswd -n 499 -s dh1357
Updating dlavigne6:
You need the response from an OTP generator.
Old secret pass phrase:
    otp-md5 8 dh0391 ext
    Response: loot omit safe eric jolt dark
New secret pass phrase:
    otp-md5 499 dh1357
    Response: hewn as dot mel mali mann
```

Sonuç

PekiOTP yine zamanlardakullanmalıyız?Uzaktakibi rbilgisayaragirdi ğinizdessh kullanıyorolaca ğınızdanvezatenshsiziniçin şifrelemei şinihallediptümileti şiminizin bu şifrelemeilegüvenli hale getirildi ğindeneminoldu ğuiçinOTP kullanmakpekiyibir fikirde ğildir.OTPdahaçokbirterminalegirdi ğinizdearkanızdan şifrenizigörebilecek olanki şileroldu ğundaiyibiryöntemolarakadlandırılabilir. İlkbakı ştabirazaçmada gelselaptopunuzlakalabalıkbiryerdeoldu ğunuzufarzedersenizçokyerindebiryöntem olduğunuanlayabilirsiniz.

Sisteminiz egirendi ğerkullanıcılarıOTP kullanmakve kullanmamak konus undaserbest bırakmakiyibirfikirolacaktır.Tabibununyanında her zamanFreeBSDsisteminizin kullanıcılarınızıOTP kullanmayazorlamasında, /etc/opieaccess dosyasınıyaratarak sağlayabilirsiniz.Fakatbununçokgüvenlibiryöntem oldu ğunusöyleyemeyiz.E ğer man opieaccessmetninebirgözatarsanızbununbirgüvenlikaçı ğıolarak kabuledildi ğini görebilirsiniz.

İyiçalışmalar.

- 1 <http://www.ietf.org/html.charters/otp-charter.html>
- 2 <http://citeseer.nj.nec.com/haller94skey.html>
- 3 <http://www.deer-run.com/~hal/ns2000/otp.pdf>

ÖzgürÖzdemircili

<http://www.enderunix.org>

<http://news.enderunix.org>

<http://haber.enderunix.org>

Sorularınızı için: dionypheles@gmx.net

Kaynaklar

DruLavigne “One-timepasswords”

FreeBSDHandbook