SelfLinux-0.12.3

Über die Sicherheit von Passwörtern

Autor: Christoph Zurnieden (*czurnieden@users.sourceforge.net*)
Formatierung: Matthias Hagedorn (*matthias.hagedorn@selflinux.org*)

Die Sicherheit eines passwortgeschützten Systems hängt entscheidend von der richtigen Auswahl eines Passworts ab. Es können im grobem fünf Sicherheitsstufen unterschieden werden: **Nachlässig**, **Niedrig**, **Mittel**, **Hoch** und **Sehr Hoch**.

Inhaltsverzeichnis

1 Über die Sicherheit von Passwörtern

Die Sicherheit eines passwortgeschützten Systems hängt entscheidend von der Wahl des richtigen Passwortes ab. Im allgemeinen unterscheidet man fünf Sicherheitsstufen: **nachlässig**, **niedrig**, **mittel**, **hoch** und **sehr hoch**.

Wahrscheinlichkeit bedeutet hier die in Prozent angegebene Wahrscheinlichkeit, mit der das Passwort in einer gegebenen Zeit durch Brute-Force-Methoden erraten werden kann. Bei Brute-Force Angriffen handelt es sich um das methodische Durchprobieren alle in Frage kommenden Schlüsselkombinationen.

Die Berechnung erfolgt nach der Formel des **National Computer Security Center [NCSC1985a]**.

$$P(S) = \frac{t_{life}\frac{n_{tries}}{\text{sec}}}{{n_c}^l}$$

Formel NCSC1985a

$$\frac{n_{tries}}{\text{sec}}$$

Dabei ist t_{life} die Lebenszeit des Passwortes in Sekunden, \frac{n_{tries}}{\text{sec}} [tfrac.png] die Anzahl der möglichen Tests pro Sekunde, n_{c} die Anzahl der möglichen Zeichen und l die Länge des Passwortes.

$$\frac{n_{tries}}{\text{sec}}$$

Der Wert von \frac{n_{tries}}{\text{sec}} [tfrac.png] liegt bei durchschnittlichen Rechnern und mit dem normalen Verfahren (crypt()) bei etwa 250.000 Versuchen pro Sekunde.

2 Nachlässig

In die Sicherheitsstufe **nachlässig** werden diejenigen Passwörter eingeordnet, die aus regulären Worten bestehen, also aus Worten, die einer Wortliste entnommen werden können. Nicht nur im Internet stehen derartige Wortlisten in großer Zahl zur Verfügung, sondern zum Beispiel auch bei Rechtschreibhilfen. Zu den regulären Worten gehören auch alle Eigennamen, insbesondere die Namen von Familienangehörigen und Haustieren. Außerdem gehören in diese Kategorie alle Worte, die auf der Reihenfolge der Tasten auf der Tastatur beruhen ("wert", "asdf" u. s. w.), sowie alle Passwörter, die schlichtweg zu kurz sind.

Wahrscheinlichkeit:
Geht gegen 100%.

3 Niedrig

Als **niedrig** gilt die Sicherheit aller Passwörter, die nach den folgenden Regeln erstellt werden:

* Das Passwort muss mindestens ein alphanumerisches Zeichen enthalten.
* Es besteht aus maximal 14 Zeichen.

* Es enthält keine Leerzeichen.
* Es kann ein Sonderzeichen enthalten.
* Es unterscheidet Groß- und Kleinschreibung.
* Es hat eine Lebensdauer von maximal einem Jahr.

Beispiele (in Klammern eine Umschreibung der englischen Aussprache):

IcvawyowgIbCic (Ic-vaw-yowg-Ib-Cic)
tunebelk (tun-eb-elk)
itvigumI (it-vig-um-I)
uccywojEgty (uc-cy-woj-Eg-ty)
hiddUlicdift (hidd-Ul-ic-dift)
SudNom (Sud-Nom)

Wahrscheinlichkeit:

10454% bei einer Länge von 6 Zeichen und einem Bestand von 65 möglichen Zeichen [a-zA-Z0-9] sowie einigen Sonderzeichen.*
161% bei einer Länge von 7 Zeichen und demselben Zeichenbestand.*
2,5% bei einer Länge von 8 Zeichen und demselben Zeichenbestand.
0,0000000000003% bei einer Länge von 14 Zeichen und demselben Zeichenbestand.

*)
Die Werte über 100% kommen dadurch zustande, dass für die Versuche die gesamte Gültigkeitsdauer zur Verfügung steht. Bei der theoretischen Anzahl von 250.000 Versuchen pro Sekunde werden die einfachen Passwörter naturgemäß sehr schnell geknackt, bei sehr einfachen Passwörter sogar deutlich innerhalb der Gültigkeitsdauer. Solche Passwort-/Gültigkeitsdauer-Kombinationen sind demnach eindeutig ungeeignet.

Das Login-Programm benutzt unter anderem auch die Möglichkeit, die Sicherheit der Passwörter durch Herabsetzung der Anzahl der Versuche pro Sekunde zu erhöhen. In den mir bekannten Distributionen ist z. B. eine kleine Pause von einer Sekunde nach Eingabe eines fehlerhaften Passwortes eingestellt. Dadurch wird die Anzahl der Versuche auf einen Versuch pro Sekunde reduziert. Dieses Verfahren sollte aber unter keinen Umständen verwendet werden, da die verschlüsselten Passwörter in einer Datei gespeichert werden.
(Es ist sehr schwierig, eine Datei so zu schützen, dass sie nicht gelesen werden kann. Es können jederzeit Sicherheitslücken auftreten, die das Lesen der Datei trotz aller Sicherheitsmaßnahmen ermöglichen, zum Beispiel durch direkten Zugriff auf die Hardware.) Auf die Angaben in dieser Datei können dann normale Crack-Programme angesetzt werden, die dann wieder 250.000 und mehr Versuche pro Sekunde erzielen können.

4 Mittel

Als **mittel** wird die Sicherheit derjenigen Passwörter eingestuft, die nach den folgenden Regeln erstellt wurden:

* Das Passwort besteht aus mindestens 8 und höchstens 14 Zeichen.
* Es kann Sonderzeichen enthalten.
* Es muss mindestens ein alphabetisches Zeichen enthalten.
* Es darf den Benutzernamen nicht enthalten.
* Es enthält keine Leerzeichen.
* Es unterscheidet Groß- und Kleinschreibung.
* Es hat eine Lebensdauer von maximal einem halbem Jahr.

Beispiel 1:

!Tvv,+I*k?%
(Sea?{~Cp@
IROKobh`#>d
vobjiWuz> (vob-ji-Wuz-GREATER_THAN)
Wruhaukbot) (Wru-hauk-bot-RIGHT_PARENTHESIS)
ishcichejKev} (ish-cich-ej-Kev-RIGHT_BRACE)

Beispiel 2 (enthält keine Sonderzeichen, die in Shellscripten Probleme verursachen könnten):

;)XbNo#h%]
j~//pdZq<
CnjKdgM(M-n*(
ofNocip} (of-Noc-ip-RIGHT_BRACE)
vafAdyif; (vaf-Ad-yif-SEMICOLON)
pomcotyadoon& (pom-cot-yad-oon-AMPERSAND)

Wahrscheinlichkeit:
0,06% bei einer Länge von 8 Zeichen und einem Bestand von 95 möglichen Zeichen [:print:].
0,0006% bei einer Länge von 9 Zeichen und demselben Zeichenbestand.
0,0000066% bei einer Länge von 10 Zeichen und demselben Zeichenbestand.

5 Hoch

Als **hoch** gilt die Sicherheit aller Passwörter, die nach den folgenden Regeln erstellt wurden:

* Es gelten dieselben Regeln wie für die Sicherheitsstufe **mittel**.
* Das Passwort muss mindestens ein numerisches Zeichen enthalten.
* Es muss mindestens ein Sonderzeichen enthalten.
* Die ersten drei Zeichen dürfen nicht gleich sein.
* Die ersten drei Zeichen dürfen nicht im Benutzernamen enthalten sein.
* Das Passwort hat eine Lebensdauer von maximal drei Monaten.

Beispiel 1:

_y@lK^T8(
`"%ld!QG2DGA

GTDeUZ#-7
IF=Qd6U*n{q
enalAjOj% (en-al-Aj-Oj-PERCENT_SIGN)
NeubOcaj< (Neub-Oc-aj-LESS_THAN)

Beispiel 2 (enthält keine Sonderzeichen, die in Shellscripten Probleme verursachen könnten):

]aj~-kn4vYc/wg
jfVN/QAfak
rVG1s<K*^5j
l=.y)Q*utZKd
udGifwis# (ud-Gif-wis-CROSSHATCH)
yewt^Shrak' (yewt-CIRCUMFLEX-Shrak-APOSTROPHE

Wahrscheinlichkeit:
Insgesamt etwas niedriger als bei der Sicherheitsstufe **mittel**.

6 Sehr hoch

Als **Sehr hoch** gilt die Sicherheit derjenigen Passwörter, die nach den folgenden Regeln erstellt wurden:

* Das Passwort muss aus mindestens 14 Zeichen bestehen.
* Es muss mindestens ein alphabetisches Zeichen enthalten.
* Es muss mindestens ein numerisches Zeichen enthalten.
* Es muss mindestens ein Sonderzeichen enthalten.
* Es muss mindestens ein Leerzeichen enthalten
* Es dürfen keine drei Zeichen in Folge gleich sein.
* Es dürfen keine drei Zeichen in Folge aus dem Benutzernamen enthalten sein.
* Die Zeichenfolge darf nicht aussprechbar sein.
* Das Passwort hat eine Lebensdauer von maximal einem Monat.

Beispiel 1:

3'cIy`a$ d\mWK(0e¤'lp
Y6E6hE®5U.Z$aQ;>|/Ps$&]R
\-IOæbq}zE&EA2
N3$a jw%{TI¢E{/%
YZ# #þ0M uyAs!'Pb
shSz*GP)1 X¾$=A(H~RXc

Beispiel 2 (enthält keine Sonderzeichen, die in Shellscripten Probleme verursachen könnten):

TIQ-Ndx¡¬O 0~]i
@6Fi=,K¹-:µ^_SG@jg~n
x)/@£z-&- _.E%_MTK2gm}5;
KmZªfc(7ÐnZziUÞR(;FQAd[r
M0 & hr}!_p14>~©KKzqaU
(R,EP md]U(Pd,A1»ZBnzi

Wahrscheinlichkeit:
0,00000000000000000013% bei einer Länge von 14 Zeichen und einem Bestand von 256 möglichen Zeichen.
0,000000000000000000000000000000000000000000001% bei einer Länge von 24 Zeichen und demselben Zeichenbestand.

(Eigentlich ist die Wahrscheinlichkeit etwas höher, da einige Passwörter entfallen. Dieser Unterschied ist jedoch nur unwesentlich.)

7 Laufzeit

Was nützt das beste Passwort, wenn es ewig haltbar ist? Je länger ein Passwort in Kraft ist, desto größer ist die Wahrscheinlichkeit, dass es doch noch geknackt, verraten oder gestohlen wird. Deshalb empfiehlt es sich, die Laufzeit von Passwörtern zu begrenzen. Je nach Sicherheitsanspruch kann eine Laufzeit von einigen Stunden bis zu einem Jahr gewählt werden. Zwischen der Lebensdauer eines Passwortes und dessen Sicherheit besteht eine direkt proportionale Beziehung. Auch ein Passwort mit der Sicherheitsstufe **niedrig** kann ausreichend Sicherheit bieten, sofern es stündlich gewechselt wird. Ebenso kann ein Passwort mit **hoher** Sicherheit durchaus Schwachstellen aufweisen, wenn es jahrelang nicht geändert wird.

Beispiel

Bei einer Laufzeit von einem Jahr besteht für ein Password der Kategorie **niedrig** mit einer Länge von 8 Zeichen eine Wahrscheinlichkeit von 2,5%, dass es innerhalb dieser Laufzeit geknackt wird. Wird die Laufzeit auf ein Monat verkürzt, so sinkt diese Wahrscheinlichkeit auf 0,2%.

Bei einer Laufzeit von einem Jahr besteht für ein Password der Kategorie **hoch** mit einer Länge von 14 Zeichen eine Wahrscheinlichkeit von 1,5e-23, dass es innerhalb dieser Laufzeit geknackt wird. Wird die Laufzeit auf ein Monat verkürzt, so sinkt diese Wahrscheinlichkeit auf 1,2e-24, also fast um das Zehnfache.

8 Extrem

Über die üblichen Sicherheitskategorien hinaus gibt es auch noch die Gruppe der **extrem sicheren Passwörter**. Dabei handelt es sich um sehr lange Passwörter, die im Normalfall niemand im Gedächtnis behalten oder von Hand eingegeben kann. Diese Passwörter werden als Schlüssel benutzt, z. B. auf elektronisch lesbaren Karten. Diese Schlüssel haben meist eine Länge von 1024 Bytes.

Hierzu ein Beispiel (der Lesbarkeit halber in ASCII-Code):

+iG8<3u9+%CY9_w5UZI6(Yt*f*DS3]&7 nHK8Z.kG^3R%jeSQB+rE ?U[,8{)boYiv!CNI"yo=5DgR/
oT%7K9u7k%o,gF>D-9cKp0[>_U='_G~l8=?E8ITdIK) iwKqB^.2u@wVKQ}7iF-0H?P"d FaqG=v4U
lx3cu.zHoo`m'}dGFx VIY%]~3mcSKkA]8)j(o&cUezo@sf\VP _W9|0{&>b?N4Ix@s;99'{PRMd~?
{r8$4Q&H9-@eKybMkZ.GW^| ^cKP{%RC`,)O^7.9>vlFa0r;:MG$V89eIssCo6*YA^U8.<<&`,YwmF@
r6z\(u%I"D^8`tY9E6YbyIX\Va<wto!0gR?N@W#3Bvz;3#s[6Umk<bf-p?M/_:g5Q3^txeW1SVmg^
KSq>Z1qNt8[SP5)zV,.nR5"F]$c`uBq!Y[wk@!5t^|&g>9p4)-yF(kosG[C%n-zI _kPAiK2&T_V{{m
\M?biIpc[1CTQOay,b ;^txeW1SVmg^KSq>Z1qNt8[SP5)zV,.nR5"F]$c`uBq!Y[wk@!5t^|&g>9p 4)-
(kosG[C%n-zI"_kPAiK2&T_V{{m\M?biIpc[1CTQOay, $d;@-mlpj&Kzj&XK\5@v@-mlpj&Kz
j&XK\5@vW,{x1,c;/$;]7w><?yN!r#$.9Xf.*d<}K -KP83~FE[TbG+2l/U~e9pGf{2Zd{}2Yp3XA^!
H0K.%/Tfr=TyQx7K0sXID}tzc;Q~E*}1a{AmQ/ITj>94Qs,RbZ/E2(zKH+(Teu<^>xXW'UEk@y,\0IA
"S4pvgC|*&7plMP5Yf?C}@C0{bkX0N<q!_ uQ6$U3s,Bmk6\V)[RhGC?7w2c*lV$i'/CWY]iVuXWYIl
E]Mz%Cq))tvU8F%<1/(<Ra!>UqKYNV)jBHW,?Tv!8&YyTPo0F}V/zV=\P>":b,i5ry~P%YW(%./;w2/
&qn;w->3,9e94qkI!Zgs9yeQbrn/SkX&WCK\K;Q,w|(G3 q{?a4cjbS$)\9eNZZ;F^7>#,mUWtQZ~Q3
:C[wiS`cDVVnWP9C(\Yhf?3IrjrX#GKfB!^;7:0/&;bq&PZHrFA8Ig!9tl;(bl#_KoufHpWM6kC"^(a
~VQ<Qh?bf@K<Md #/0Uep@`|T/KI(f^/c9 WA"G1NV(I}_

Der entscheidende Nachteil solcher Schlüssel besteht darin, dass man sie schriftlich festhalten muss. Es besteht zwar die Möglichkeit, diese Schlüssel mit einem normalen Passwort zu kombinieren. Dies bring allerdings keinerlei Vorteile mit sich, sondern erhöht die Gefahr eines allzu sorglosen Umganges mit dem Passwort.

Alle hier angeführten Beispiele wurden mit dem **Automated Password Generator** (`apg`) von *Adel I. Mirzazhanov generiert*, den Sie unter  http://www.adel.nursat.kz/apg/ finden. In der hier verwendeten Version 2.0.0 final PRNG: X9.17/CAST) generiert dieses Tool allerdings weder Leerzeichen noch Zeichen oberhalb von 128 dezimal. Sofern diese Zeichen in den Beispielen vorkommen, wurden sie per Hand eingefügt.

9 Fazit

Wie man anhand der in diesem Abschnitt aufgelisteten Wahrscheinlichkeiten sieht, reicht schon der regelmäßige Wechsel eines sorgfältig gewählten Passwortes mit einer Länge von 8 Zeichen aus, um eine relativ hohe Sicherheit zu erzielen.