COMPUTERWORLD

Gode passwords, hvad er det

Hvordan vælger man gode passwords, Hvordan virker et cracker værktøj og hvor lang tid tager det at cracke et password. Råd og vejledning om passwords som du kan bruge til at forklare dine brugere hvorfor passwordet er vigtigt

Skrevet den **12. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Gode passwords, hvad er det??

Nu kunne det måske se ud som at dette er en relativ ny artikel, hvis du kikker på datoen i højre øverste hjørne. Det er det ikke , det er en artikel fra januar 2004 (se de ældste kommentare) der er blevet rettet op med nye password længder så den lever op til nutidens krav

De fleste netværkssystemer baserer deres sikkerhed på kombinationen af password og brugernavne, hvor brugernavnet vælges af netværkets administrator og passwordet at brugeren. Hvilket password brugeren vælger, er af afgørende betydning for sikkerheden. Nedenstående råd bør følges, da de giver høj grad af sikkerhed og ikke koster penge.

Regel nummer 1: "Et password skal kunne huskes"

Følgende bør undgås:
1. Man må aldrig bruge brugernavnet eller dele heraf.
2. Man må aldrig bruge sit eget fulde navn eller dele heraf.
3. Man bør ikke bruge ord der står i en ordbog, slet ikke en engelsk ordbog.
4. Man bør ikke bruge navne eller numre, der kan forbindes med brugeren, f.eks. tlf. numre fødselsdage og børnenavne.
5. Man må ikke bruge logiske tastkombinationer f.eks. qwerty
6. Et password må aldrig skrives ned.
7. Man bør ikke bruge æ,ø, å, punktum, komma og tankestreg
8. korte passwords under 10 tegn

Forklaringen på at æ,ø og å ikke bør anvendes er egentlig relativ simpel og lige for. Hvis man arbejder i server miljøer, er operativsystemer altid engelsk, hvilket kan give problemer, især ved konverteringer til nyere versioner. Den vigtigste grund er at men ved nedbrud, nogle gange står med et system, der kun har engelsk tastatur. Hvis man så har brugt danske karaktere til f.eks. administrator kontorn, kan dette faktisk betyde, at man ikke kan logge på, og dermed ikke kan redde sin data. Det giver selvfølgelig et rigtigt sikkert system, men man får ikke ros når firmaet midster alt sin data eller skal have fat i en dyr løsning for at genskabe det.

Følgende bør vælges
1. passwordet bør være mindst 10 tegn langt men gerne 14 eller længere.
2. Et password bør indeholde både små og store bogstaver samt tal og specialtegn.

Sådan virker et passwordcracker værktøj.

Når du taster et password ind i Windows, bliver dette password konverteret til en såkaldt Hash Værdi (i virkeligheden er række bits, ofte 160, skrevet med hexadecimale tal, værdier fra 0 til F).

En hash værdi er kendetegnet ved at to forskellige passwords ikke kan give den samme hash værdi og ved at du ikke kan regne baglæns og ud fra en hash værdi kan regne dig frem til passwordet.

Password cracker værktøjer kan med andre ord ikke regne sig frem til dit password, den kan kun prøve sig frem med forskellige passwords som den omsætter til hashværdier, som den derefter sammenligner med hash værdien fra dit password og hvis de to hash værdier er ens, vil passwordene også være det, hvilket betyder at dit password er cracket.
Passwordcrackerværktøjer fungere på den måde, at de fra starten indeholder en liste over hashværdier på de mest almindeligt brugte ord og tast kombinationer. Når værktøjet indlæser hash værdierne fra din maskine, vil det genkende alle de hash værdier, og deres tilhørende passwords, hvor brugeren har brugt et kendt ord eller tastekombination. Dette tager 0 sekunder, hvorfor sådanne passwords selvfølgelig er værdiløse, Se eksemplerne herunder).
Passwordcrackerværktøjer indeholder også en ordbog, der kan skiftes af hackeren. Som default indeholder de normalt en engelsk ordbog, men en dygtig hacker vil skifte denne ordbog med ordbøger specielt tilpasset til de forhold han forventer at møde. I danmark vil man således indlægge en dansk ordliste, en engelsk ordliste, en liste over danske pige og drenge navne, samt en liste med ord der høre til det firma/organisation man ønsker at angribe.
Ordene i ordlisterne omsættes til hash værdier, der sammenlignes med de indlæste værdier, og hver gang to ens findes er et password cracket. Hvis du synes dette lyder som en langvarig proces, så se eksemplerne herunder.
Den sidste metode der gennemføres, kombineres med ordliste og er således faktisk to metoder. Metoden kaldes Brute Force, og er en systematisk afprøvning af alle kombinationer af små bogstaver, små og store bogstaver, små, store bogstaver og tal, små, store bogstaver, tal og special tegn. Først brute forces i kombination med ordlisternes ord. D.v.s. kombinationer af bogstaver, tal, og tegn stilles foran og bagefter ord fra ordlisten hvorefter der forsøges med ren Brute Force.
Parewordcrackeværktøjet kan selvfølgelig konfigureres på et væld af måder. Du kan indstille hvor lange ord den skal forsøge med, om den skal forsøge med både store og små bogstaver, tal og tegn, og meget mere.

Eksempler på hvor hurtigt passwords kan cracker.
Nedenstående liste er lavet med cracke programmet L0phtCrack 4.0, og er selvfølgelig berbejdet, bl.a. er brugernavnene fjernet, og da listen fyldte 14 sider er kun udvalgte eksempler medtaget. L0phtCrack er ikke konfigureret, ordlisten er den medfølgende standard engelske ordliste, Computeren er en 533 Mhz pentium, der lavede andet mens den crackede. På en ny PC, med konfiguration og en dansk ordliste, vil man kunne dividere tiderne med en faktor 5.

"brugernavn"	0 sek	
111111	0 sek	Ordliste
123123	0 sek	Ordliste
123456	0 sek	Ordliste
654321	0 sek	Ordliste
MICHELLE2	10 sek	Hybrid
MUSTANG94	10 sek	Hybrid
BRAVO7	22 sek	Hybrid
BRIAN0405	22 sek	Hybrid
DEXTER3	37 sek	Hybrid
DIANA0105	37 sek	Hybrid
COMMUNICATION3	1 min 20 sek	Hybrid
POLAR1	1 min 20 sek	Hybrid
MMMMMM	10 min 44 sek	Brute Force
MANDAG	11 min 38 sek	Brute Force
METALSTORM	46 min 51 sek	Brute Force
KALTOFTIDA	49 min 27 sek	Brute Force
SKOVBRYNET42	5 timer 41 min 34 sek	Brute Force

```
TIGERDYR2           5 timer 43 min 56 sek      Brute Force
O6VQ2U8O5LIQR6     12 timer 12 min 19 sek      Brute Force
LONNI48            12 timer 19 min 13 sek      Brute Force
```

Nu kunne du måske fristes til at tro at LONNI48 er et godt password, når det tager hele 12 timer og 20 minutter, men deter det ikke, et godt password bør tage mindst 3 måneder at cracke (da man, hvis man arbejder i et sikkert system, skifter password mindst hver 3. måned)

Hvordan laver du gode passwords der kan huskes:
Giv specialkarakterene navne og lav rebuser, se nedenstående eksempler:
"jeg bor i huset ved de 2 hvide norske havelåger" = jbihvd2hN#
"Andresine og hendes 3 nevøer Rip, Rap og Rup samt Anders" = &oh3nIAUsA
"hos Lonni og Frank finder du 3 hvide katte + Fido" = @LoFd3hk+F
"dykkeren Søren fandt 25 gamle Tyske søminer i havet" = dSf25gT¤ih

Kommentar af janbb d. 31. Jan 2004 | 1

loppiuyt88*;)

Kommentar af nuna d. 23. Mar 2004 | 2

Kommentar af cms d. 17. Jan 2004 | 3

Overraskende god

Kommentar af tommyf d. 16. Feb 2004 | 4

Sjovt med forslagene til sidst. Ville dog gerne have forklaret hvorfor æøå ikke bør bruges, alt andet lige er de fleste hackerværktøjer vel amerikansk/engelsk og tilbyder derfor kun mulighed for a-z. Så burde et enkelt æ udlukke de fleste scriptkiddies?

Kommentar af hermandsen d. 22. Jan 2004 | 5

Kanon artikel!! Intet mindre!! Tror vores administrator her ude ville blive glad for at hænge et par eksemplare op rundt omkring!! ;)

Kommentar af karsten_larsen d. 27. Jan 2004 | 6

Gode fif til gode password

Kommentar af ysubhi d. 15. Oct 2004 | 7

kanont

Kommentar af iphase d. 21. Jan 2005 | 8

Jeg vil lige tilføje at det heller ikke er en dårlig ide med sætninger, det har jeg stor succes med hos mine brugere. eks.
"Min kat er #1". på denne måde opnår man hurtigt et langt antal karaktere i sit password, og bruger mellemrum som er et special tegn mange hacker værktøjer ikke lige kan forholde sig til.

Kommentar af donslund d. 18. Jan 2005 | 9

En fornugtig artikel der er nemt at forstå.

Kommentar af m-koldsgaard d. 16. Jan 2004 | 10

Fin artikel

Kommentar af locturian d. 11. Aug 2004 | 11

God artikkel, som alle bør læse :) Ikke fordi man i min branche ikke ved det i forvejen, men problemer opstår som regel når slutbrugeren ikke ved disse ting, og har et password der enten er cpr nummer, eller navnet på katten... Thumbs up

Kommentar af athlon-pascal d. 16. Jan 2004 | 12

Du gjorde det igen! - en ting der dog undrer mig: "7. Man bør ikke bruge æ,ø, å, punktum, komma og tankestreg" - er æ, ø og å dårligere end f.eks. a?

Kommentar af crazy_legs d. 31. May 2005 | 13

Kommentar af rigtigmmk d. 15. Jan 2004 | 14

Godt artikel bufferzone.

Kommentar af rocekiller d. 05. Jul 2005 | 15

Lidt kort. Mest om et windows password-cracker værktøj, for lidt om passwords. Hele sætninger kan klart anbefales hvor systemet understøtter det, specielt hvis man er hurtig på tastaturet.

Kommentar af cronck d. 30. Mar 2005 | 16

Blev ikke selv meget klogere, men mange kan helt sikkert bruge dette!

Kommentar af hejhej (nedlagt brugerprofil) d. 23. Jan 2004 | 17

God artikel :o)

Kommentar af rudi1234 d. 23. Sep 2004 | 18

Kommentar af ellegaarddk d. 13. Jun 2004 | 19

Toltalt uening i at man ikke skal bruge øæå. Hvis ellers systemet kan håndtgere det udelukker det næsten automatisk muligheden for at finde noget som helst med et cracker værktøj med en engelsk ordbog.

Kommentar af ravsted_dk d. 26. Jan 2004 | 20

Kommentar af googolplex d. 10. Feb 2005 | 21

Kommentar af drengen1987 d. 09. May 2005 | 22

Vidste ikke at hackerens værktøjer var så gode...

Men det ved jeg heldigvis nu...

Kommentar af lordhead d. 21. Jan 2004 | 23

/Lordhead ;)

Kommentar af htmlkongen d. 19. Jan 2004 | 24

God artikel Buff ;)

Kommentar af daxthevaks d. 23. Mar 2004 | 25

Kommentar af madsass d. 11. Dec 2004 | 26

Kanon artikel.

Kommentar af baxos d. 15. Jan 2004 | 27

Igen meget nice artikle! Keep on good working :)

Kommentar af ttj d. 18. Jan 2004 | 28

Endnu en god artikel!

Kommentar af m0nk3y d. 01. Apr 2005 | 29

Rigtig god artikel! Lang tid siden jeg har mødt en der var så god til at skrive, og stadig så stabil omkring din viden om computer :)

Kommentar af squashguy d. 15. Jan 2004 | 30

Jeg må give bufferzone ret.. stærke passwords er ekstremt vigtige, hvis en hacker har mulighed for at få fat i filen med passwords/sniffe over netværk, og kan lave brute forcing.

Kommentar af dart d. 13. Nov 2005 | 31

Kommentar af xxgullexx d. 12. Dec 2004 | 32

Aha! Sejt... jeg vil finde nye passwords på den beskrevne måde!

Kommentar af da9el d. 12. Feb 2005 | 33

Kommentar af talant d. 25. Feb 2004 | 34

God artikel som alle faktisk bør læse..

Kommentar af don_q d. 11. Oct 2004 | 35

Kommentar af ejvindh d. 11. Aug 2004 | 36

Det er en rigtig god artikel, idet den demonstrerer HVORFOR nogle passwords er ubrugelige - nemlig fordi hacker-programmerne "kender" dem.

Kommentar af wanze d. 22. Jul 2004 | 37

Ville også gerne vide hvorfor Æ, Ø og Å ikke burde benyttes.

Kommentar af sorenbs d. 12. Jan 2005 | 38

jada

Kommentar af taub d. 02. Jun 2005 | 39

God artikel... Let fordøjelig, og godt skrevet.
Sidder man med et web-site med en login-side der skal beskyttes, kan man fx begrænse hvor mange gange som dagen en bruger kan taste et forkert password ind, og derved forlænge cracking-processen mange gange. Man kan også vise et dynamisk genereret billede, med en tilfældig kombination af tal og bogstaver, som brugeren skal taste ind i et 3. felt, hvis passwordet var forkert fx 3. gange. Denne metode ses efterhånden mange steder på nettet, efter min erfaring.

Kommentar af crybet d. 12. Aug 2004 | 40

Kommentar af bjerregaard d. 31. May 2005 | 41

Kommentar af tuekappel d. 05. Jun 2005 | 42

En rigtig god artikel, som jeg vil læse op for mine kolleger. Mit firma har adgang til sin egen server via VPN, over internettet, og mine kolleger FATTER ikke hvorfor det er vigtigt at have et kompliceret password. Jeg mener, en af dem skrevt til mig over messenger "er vores password ikke (indsæt kompliceret password)?" Jo, makker, og nu er vi nødt til at skifte det IGEN!
Jesus, the stupidity we have to put up with...!

Kommentar af kta38 d. 31. Dec 2005 | 43

Oki.

Kommentar af cram d. 22. Mar 2006 | 44

Totalt iorden mega fed havde faktisk lige brug for det :P

Kommentar af kristo89 d. 13. Oct 2006 | 45