COMPUTERWORLD

PasswordHacking med Rainbow Crack

Windows passwords er døde. Selv de bedste passwords kan crackes på få minutter. Rainbow Crack er et spændende projekt der allerede nu rykker ved sikkerheden og stiller nye krav til os som administratorer.

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Kryptering** | ★★★☆☆

Rainbow Crack - Speed til hackerne
http://www.antsight.com/zsl/rainbowcrack/

Våbenkapløbet døde ikke med den kolde krigs afslutning, og den har aldrig været begrænset til den militære verden. Også i IT verdenen har den kørt løbende gennem årene som et kapløb mellem TI sikkerhedsbranchen og hackerne. Rainbow Crack lyder måske nok som narkotika, men I virkeligheden er det blot endnu kapitel den fortsatte føljeton om kampen mellem password sikkerhed og cracker værktøjerne. Lige nu er de sidste desværre foran.

Windows Password - Sådan virker det
Når du taster et password ind i din Windowsmaskine første gang, omsættes det automatisk til en såkaldt hashværdi (Endnu en narkotisk reference, der i virkeligheden intet har med narko at gøre. Husk at computerens fædre for størstedelens vedkommende er fra 68 generationen. Det kunne jo forklare en del). En hashværdi er en streng af hexadecimale værdier.

http://www.fileformat.info/tool/hash.htm

```
Prøv f.eks. med ordet "eksperten" (uden " selvfølgelig)
Original bytes     65:6b:73:70:65:72:74:65:6e (length=9)
Adler32          130803d2 CRC32 da4228c4
Haval          dffd21694a46c050ec12d494e98cf63e
MD2          5b57cdb3a506bea2b55ff54cf15a37d7
MD4          d3162e7d9af7ac12c36676bc74abe7c1
MD5          2b12d915e46ec434d5cf1a40eadb643a Ripe
MD128          5196eca984f67370832824afb18e6ea4 Ripe
MD160          70ad85695a095d0f87e9eb3281bbb06897e745f9
SHA-1          7cfa3926bf32946932e8a9eeac983a40a5167b19
```

Ordene til højre i boksen er forskellige algoritmer, strengene til venstre er hash værdierne

Den genererede hashværdi gemmes af Windows i SAM databasen og det password du har indtastet dumpes. Det er således ikke passwordet der gemmes på maskine, men ordets hashværdi og når du igen taster dit valgte password ind under logon til Windows, laves det indtastede ord om til en hash værdi, der så sammenlignes med den værdi Windows har gemt i databasen.

L0phtcrack - Sådan virker et password crackeværktøj

Som eksempel kunne vi jo kikke på L0phtcrack der nok er det kendteste værktøj af slagsen. Værktøjet arbejder med SAM databasen, som du kan indlæse i forskellige former alt afhængig af hvordan du har fået fat i den. L0phtcrack kan håndtere SAM Databasen både i sin originale form som den f.eks. findes på en rescue diskette, eller i tekst form som du ville have den, hvis du havde hacket dig til den f.eks. med et værktøj som PWDump.

Du har også mulighed for at læse en ordbog og jo bedre denne (eller disse) ordbog (bøger) er, jo flere ord og jo hurtigere kan L0phtcrack cracke passwordene til dig. Ordbøger findes i mange forskellige versioner og sprog på nettet og normalt vil en hacker arbejde med intelligent sammensatte samlinger af ordbøger indeholdende en stor ordliste på landets sprog, en navneliste med populære pige og drengenavne, en engelsk ordliste, en ordliste med meget brugte passwords og taste kombinationer og en liste med branche specifikke ord alt efter hvorfra den SAM database han forsøgte at cracke kommer fra.

Når du så starter L0phtcrack er det første den gør at sammenligne de hash værdier den finder i den indlæste fil med en indbygget liste af meget (rigtig meget) populære ord og tastekombinationer. Hvis der brugere der har brugt disse ord eller tastekombinationer, f.eks. qwerty, så cracker L0phtcrack ikke hachværdien, den genkender den simpelthen umiddelbart og udskriver passwordet med en tidsangivelse på 0 sekunder.

Næste trind er at L0phtcrack omregner ordene i ordbogen (L0phtcrack betragter de indlæste lister som en ordbog) til hashværdier og sammenligner dem med de indlæste værdier en af gangen. Har dine brugere anvendt ordt der findes i ordbogen, vil deres password blive fundet i løbet af 0 sekunder til 15 til 20 minutter, alt afhængig af hvor stor ordbogen er, hvor hurtig computeren er og hvor mange passwords den skal sammenligne med. Denne metode kaldes Dictionary Attack.

Når ordbogen er kørt igennem, vil L0phtcrack forsøge en gang til med alle ordene. Denne gang sættes forskellige kombinationer af tal og tegn før og efter ordene. Det er meget almindeligt at folk laver password med tal i enden for at kunne nøjes med at ændre tallet næste gang de skal skifte password, så det bliver lettere at huske. Et typisk password af denne type, kunne være eksperten05 og et sådant vil blive fundet i løbet af 15 minutter til 2 til 5 timer alt afhængig ..... Denne metode kaldes Hybride Attack.

Sidste metode kaldes for Brute Forcing, og her laver L0phtcrack alle mulige kombinationer at tegn, tal og specialtegn. Brute Forcing er meget tidskrævende og hvis du har brugt meget lange password, f.eks. 14 karakterer, med både store og små bogstaver, tal og specialtegn vil denne metode tage mange år at gennemføre og er dermed ikke praktisk gennemførlig.

L0phtcrack brugbarhed i dag.
Når nu et ordentligt password kan tage mange år at cracke, kan man så overhoved bruge et værktøj som L0phtcrack?
Svaret er desværre ja, og grunden er folks manglende forståelse for hvorvor de skal bruge gode passwords og hvad et godt password er. Hvis du laver øvelsen med L0phtcrack skal du ikke blive forbavset, hvis værktøjet har fundet en tredjedel af dine password på under 2 timer hvis du ikke enforcer stærke passwords.

Rinbow Crack forklaret.
Vi starter her med lidt fine ord, som nok skal blive forklaret. Rainbow Crack bygger på Faster Time-Memory Trade-Off Technique og er udviklet af Philippe Oechslin på baggrund af tidligere arbejde af Hellman (bl.a. kendt fra Diffie-Hellman algoritmen der anvendes af IPSec VPN).

Og så på dansk. Rainbow Crack er et Dictionary Attack, der I virkeligheden bygger på gamle teknikker sat sammen på en ny made.

Først har man lavet en database med alle de ord, eller rettere tegnkombinationer, det er muligt at lave med alle små bogstaver, alle store bogstaver, alle tal og alle specialtegn fra ord på et bogstav (tegn) op til 14 bogstaver (tegn). Og hvis du nu tænker for dig selv "Det må godt nok være en stor database" så har du

ganske ret, den er enorm.

Dernæst har man udregnet alle Hashværdier og indskrevet dem i databasen. Og hvis du nu tænker for dig selv "Det må godt nok have taget lang tid" så har du ganske ret, de er, som jeg forstår det, ikke helt færdige endnu.

Til sidst, har man distribueret databasen ud på Internettet til flere hosts for på den måde at gøre hele systemet hurtigere.
Når du indlæser en hashværdi der skal Crackes, skal man "bare" finde din hashværdi i databasen og udlæse det ord der har givet hashværdien.

Man udnytter, at den tid det tager at udregne hashværdien kun skal betaler en gang, hvorefter det bare er et spørgsmål om at finde resultatet og det er mange gange hurtigere. Rainbow Crack påstår at de kan cracke ethvert Windows password på 14 tegn og ned, på under 4 minutter.

Windows password beskyttelse er død, hvad gør vi nu
Hvis du nu er lidt i vildrede men om det overhoved kan betale sig at bekymre sig om password, og det kan betaler sig at lave gode passwords og enforce stærke passwords, så er svaret stadig ja.
For at kunne cracke dine passwords, skal hackeren stadig have fat i hashværdierne som findes i SAM databasen, og så skal han jo ind på din maskine og have rettigheder til at kunne tilgå dem og få dem med ud.
Det bliver med andre ord endnu mere vigtigt at holde hackeren ude af dit system i første omgang og det bliver endnu mere vigtigt at sikre systemerne, så de kritiske ting på vores systemer bliver endnu mere utilgængelige end før.

tiden efter Rainbow Crack
Rainbow Crack er under udvikling i øjeblikket og det er planen at den på sigt skal blive en betalingstjeneste. Dette betyder dog ikke at den ikke vil blive brugt til slemme ting, princippet er nu bevist og andre kan lave samme tjenester og systemer i det skjulte. Selv programmet L0phtcrack kan tilsyneladende anvendes sammen med Rainbow Crack, og @stake der haar udviklet L0phtCrack er for relativt nyligt blevet købt af Symantech. Hvad dette opkøb udarter sigtil vides pt. Ikke.

Der er også løsninger der kan og vil afløse/udbygge det traditionelle Windows passwords. Her er lidt forskelligt:

Two factor security/Authentication. Her kombinerer man noget man ved (f.eks. et password) med noget man har (f.eks. en sikkerheds token) eller med noget man er (også kaldet biometrics, f.eks. fingeraftryk scanning eller iris scanning).

Dynamic algoritms kunne være en anden løsning. Her genereres algoritmen dynamisk under installation, således at den algoritme der generere hashværdien på de forskellige computere og netværk er forskellig. Dermed skal der laves en Rainbow Crack directory for hver mulig algoritme, og det er ikke muligt. Jeg forestiller mig f.eks., at man under installation først afkræves et password eller sætning, der bruges til at generere algoritmen, hvorefter man opgiver sit logon password, der så hashes med den algoritme der er genereret på maskinen.

Hvis du har spørgsmål, bemærkninger eller tilføjelser så hører jeg gerne fra dig på kim@bufferzone.dk eller på eksperten hvor jeg ofte er til at finde. Jeg beder om at du ikke stiller spørgsmål i artiklens kommentarer da jeg her ikke kan svare på dem. Hvis du bidrager med en tilføjelse, vil du naturligvis blive nævnt sammen med din tilføjelse.

Kommentar af simm d. 27. Feb 2006 | 1

Spændende læsning :)

Kommentar af jps6kb d. 01. Dec 2005 | 2

Alletiders :)

Kommentar af martin1000ben d. 02. Mar 2006 | 3

Kommentar af apj d. 30. Nov 2005 | 4

Fint. Lidt kort, men stadig ok.

Kommentar af the_email d. 29. Nov 2005 | 5

Vældig spændende artikel

Kommentar af master-lion d. 07. Dec 2005 | 6

En god artikel :-)

Kommentar af cronck d. 01. Dec 2005 | 7

Er godt nok overrasket over at det kan lade sig gøre på så kort tid. Kanon artikel!

Kommentar af humpfrey d. 24. May 2006 | 8

Kommentar af fromsej d. 29. Nov 2005 | 9

Flot og gennemarbejdet som sædvanligt.

Kommentar af mezoi (nedlagt brugerprofil) d. 20. Jan 2006 | 10

Kommentar af truelz d. 05. Dec 2005 | 11

Gyseligt... Altså metoden du redegør. Artiklen fejler ikke noget. En god grund til at fjerne "Users"-gruppens read access på alle drevene :-)

Kommentar af dreamless d. 01. Dec 2005 | 12

God artikel men stavefejlene kan gøre det lidt forvirrende at forstå.

Kommentar af per-olof d. 01. Dec 2005 | 13

Meget intresant og go artikel

Kommentar af bodyguard d. 14. Feb 2006 | 14

Kommentar af dustie d. 29. Nov 2005 | 15

Som altid godt skrevet.

Kommentar af nielle d. 28. Jan 2006 | 16

To the point

Kommentar af the_ghost d. 29. Nov 2005 | 17

Igen igen - En spændende og interesant artikel, som man bare bliver nød til at læse færdig.

Kommentar af madshammer d. 26. Jan 2006 | 18

Kommentar af vallemanden d. 12. Nov 2007 | 19

Kommentar af swiatecki d. 29. Nov 2005 | 20

Jeg lærte en hel del.. og godt forklaret

Kommentar af hanne_e d. 30. Nov 2005 | 21

Kommentar af simonhans73 d. 17. Feb 2006 | 22

Kommentar af psycosoft-funware d. 30. Nov 2005 | 23

mange af tingene kendte jeg godt til inden jeg læste artiklen, men for "newbies" er det en super god artikel - rigtigt godt skrevet og gennemarbejtet :-)

Kommentar af mtj111 d. 30. Nov 2005 | 24

Meget god artikel, som giver en god og let forståelig forklaring på L0phtcrack og Rainbow Crack!

Kommentar af cpn80 d. 01. Dec 2005 | 25

Så blev jeg det klogere. Jeg takker 8)

Kommentar af l0gical d. 23. Feb 2006 | 26

Kommentar af there-is-only-xul d. 30. Nov 2005 | 27

nice1, som altid :)

Kommentar af datasource d. 30. Nov 2005 | 28

super !

Kommentar af halllah d. 29. Nov 2005 | 29

Kommentar af vemo d. 30. Nov 2005 | 30

Udemærket artikel - dog havde jeg håbet på et lidt højere teknisk niveau.
Iøvrigt syntes jeg at man burde checke for stavefejl på artikler man skal betale point for at læse...

Kommentar af lassemelbye d. 07. Jul 2006 | 31

Rimelig nice, ikke bare for hackning, men også for sikkerhed

Kommentar af kingzicz d. 24. Feb 2008 | 32

fin artikel (:

Kommentar af superfisker d. 09. Jul 2008 | 33

Super artikel !