COMPUTERWORLD

Hackernes værktøj nr. 1, Google

Mange tror at hackerne betjener sig af obskure værktøjer, der er skrevet med hemmelige besværgelser i mørke kældre en sen nattetime af andre onde hackere. Dette er langt fra tilfældet. De fleste af de værktøjer der anvendes til hacking er ganske almindeli

Skrevet den **04. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Formålet med artiklen er ikke at undervise I hacking, men at gøre webmastere og netværksadministratorer opmærksom på hvor meget Google faktisk kan afsløre af fortrolige og potentielt belastende oplysninger, samt give nogle bud på hvordan man tester sine egne sites for disse ting samt fjerner problemerne når man finder dem. Alle artiklens informationer og beskrivelser er frit tilgængelige på bl.a. Google.

The G00gle Attack Engine.

Google er en genial søgemaskine, der bruges af stort set alle mennesker. De fleste nøjes med at indtaste enkelt ord eller mindre sætninger og så lede efter et resultat der kan bruges mellem de første 3 sider. Google indeholder dog nogle meget avancerede muligheder for at forfine sin søgning og hvis man kombinere disse avancerede muligheder med viden om hvad man skal søge efter kan Google faktisk blive et utroligt stærkt værktøj for en hacker.

Lad os starte med at kikke på nogle af de avancerede muligheder Google giver os:

Læs mere her:
Google's Advanced Search page. http://www.google.com/advanced_search
Google Advanced Search Operators page. http://www.google.com/help/operators.html
Idrada's artikel "Google for videregående". http://www.eksperten.dk/artikler/61

Hvis du starter med at indtaste et ret almindeligt ord som f.eks. "budget" i google vil du få over 35.900.000 hits, ikke særligt brugbart eller præcist og sandsynligheden for, at du finder det du leder efter er lille. Med operatoren "filetype" kan du specificere hvilken type fil, du leder efter og selvom Advanced Search page lister flere almindelige formater som f.eks. Microsoft Word, Microsoft Excel, and Adobe Acrobat PDF, så kan du sagtens søge efter flere formater end disse, hvilket vi vil udnytte senere. Prøv nu at søge i google med "budget filetype:xls" (uden ") du er nu nede på ca. 79,400 hits, stadig alt for mange, men dog betydeligt bedre end før.
Vi kan nu prøv at tilføje endnu en operator i vores forsøg. "site" operatoren giver dig mulighed for at gennemsøge et specifikt site. Prøv f.eks. med denne søgning "site:www.securityfocus.com password cracking" som giver dig 465 resultater fra et hardcore site når vi taler om computersikkerhed. Faktisk kan du med fordel bruge denne metode til at søge et site igennem selvom sitet selv tilbyder en site-search, ofte er Google bedre, og ud fra et hacker synspunkt, så finder du flere interessante ting med Google end med den søgemulighed sitets egen webmaster har stillet til rådighed. . "site" operatoren er ikke begrænset til komplette sites, men kan også håndtere domæner, herunder toplevel domæner f.eks. "site:dk", der gennemsøger alle dk sites.

Og lad os så begynde på hackingen:

Med "intitle" operatoren kan du søge efter sider der har et bestemt ord I deres title. Hvis du f.eks. søger med "site:www.securityfocus.com intitle:password cracking" (bemærk her at det kun er ordet password, der skal stå I titlen. Ordet Cracking skal bare findes på siden).
Intitle opratoren i sig selv er ikke farlig, men hvis man kombinerer den med anden viden kan den udnyttes. Mange webservere er konfigureret til at vise mappe indholdet hvis der ikke findes en default Web page (index.htm eller default.htm) I biblioteket, og det kan udnyttes. Titlen på disse sider er næsten altid "Index of", så prøv at søge med " intitle:"index of" site:edu password ". Omkring 2.930 resultater af hvilke de fleste er værdiløse for en hacker, men mange vil give dig passwordlister i klar tekst og andre vil give dig filer der kan crackes med frit tilgængelige værktøjer, hvis du ved lidt om hvilke filer der typisk indeholder passwords. Med en lille smule fantasi kan du sikkert selv finde på at prøve med ord som passwd. htpasswd. accounts. users.pwd. web_store.cgi. finances. admin. secret. fpadmin.htm. credit card. ssn. bash. History. Temporary. password. Og så videre.
Hvis du har viden om hvilke scripts og utilities hackerne typisk bruger, kan du søge med " intitle:"index of" programnavn " og dermed finde alle de sites hvor hackere har gjort arbejdet for dig og placeret programmer der kan give adgang eller mulighed for at styre en webserver remote.

Operatorerne allinurl og inurl kan vi arbejde med selve url'en og dermed med kendte stier på web serveren og dermed snævre søgningerne ind. Brugbarheden af disse to operatorer afhænger stærkt af din viden. Både web servere, forskellige webfora og andre web værktøjer anvender faste stier og kendskab til hvor de default placerede interessante oplysninger kan hjælpe. Prøv f.eks. at søge med " inurl:sitebuildercontent", " inurl:sitebuilderfiles" eller " inurl:sitebuilderpictures", der udnytter default placeringer af filer i Sitebuilder Web Design program. "allinurl:auth_user_file.txt" der udnytter default placeringerne for DCForum and for DCShop (Shopping cart program) passwords (hashede, men kan crackes relativt let). Af andre meget anvendelige operatorer kan nævnes allintext og intext samt inanchor og allinanchor. Hvad disse 4 operatorer kan anvendes til, kræver ikke megen fantasi, men dog lidt viden om hvordan de mest anvendte web løsninger er skruet sammen.

Hacking af kritisk hardware eller det der er værer!:

Meget forskelligt hardware administreres i dag via et web interface. Dette betyder at du kan bruge google til at finde ubeskyttet hardware hvis du ved lidt om hvordan web interfacet virker.
Prøv f.eks. søgningen " inurl:"ViewerFrame?Mode=" " , " inurl: "MultiCameraFrame?Mode=" " eller " inurl: "axis-cgi/mjpg" " disse vil give dig flere hundrede eksempler på overvågnings web kameraer der ikke er beskyttet godt nok (ser flere eksempler på forskellige søgninger her, der er ganske mange http://www.undertree.us/allcams.html).
I første omgang virker det måske relativt harmløst, at vi kan sidde i Danmark og kikke på andre personers mere eller mindre offentlige web cam's, men hvis du kan finde kameraets IP adresse med google, kan det også hackes og det kan have nogle uheldige konsekvenser.
Hvis der f.eks. er tale om et overvågnings kamera der er en del at tyverisikring af et firma eller et privat hjem, kan man måske SYN floode kameraet eller lave andre former for DOS angreb, så kameraet ikke virker når indbruddet sker, eller de kan bruges til at kontrollere om der er nogen hjemme og om der er noget der er værd at stjæle.

Mange af disse kameraer har både indbyggede web servere og indbyggede SMTP servere (til udsending af still fotos som en del at deres overvågnings kapacitet). Kan disse servere hackes, kan de f.eks. bruges som Mail relay's til udsending af spam, defacing og andre ting du måske ikke har lyst til at deltage i.
Nu har jeg cirklet lidt om web cam's, men det samme er muligt med flere andre forskellige enheder, f.eks. printere, routere hvis der ikke er sat nogen form for filtrering op eller hvis de er fejlkonfigurerede, firewall's hvis de er fejlkonfigurerede. Faktisk er det kun fantasien der sætter grænsen, både for hvilke enheder der kan udnyttes og for hvad der kan gøres med dem

ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL ADVARSEL

Hvis du ikke har meget styr på disse værktøjer, skal du være meget forsigtig med at tilgå dem hvis du finder dem. En del hackere laver fake exploits, der ligner de rigtige værktøjer, og når du dobbeltklikker dem, vil de placere bagdøre eller gøre andet potentielt grimt ved din maskine, så vær aldrig ukritisk når du arbejder med den slags værktøjer.
Jeg tester selv alle værktøjer og exploits i et lukket miljø, hvor jeg kan holde øje med hvad der sker og med om maskinen kommunikere ud.
Hvis du finder følgende programmer og scripts i dine egne web biblioteker, bør du reagere: cmd.exe (dette program har du på din maskine, men det bør aldrig findes i web biblioteker, med mindre du selv har placeret det der og ved hvorfor), cmd.asp, cmd.php, nc.exe, m.m.

Hjælp til at finde sårbarheder og fortrolige informationer.

Der findes faktisk sites der har gjort det til deres mission at finde sites der udstiller deres uvidenhed og fortrolige informationer. Googledorks http://johnny.ihackstuff.com/index.php?module=prodreviews er en at de bedste, prøv selv og se om dit site skulle være at finde her. Lidt analyse af de ting Googledorks finder kan også give dig et godt billede af hvad du skal kikke efter, og er du en haj til f.eks. Perl og kender Google's Web API, kan du faktisk selv lave scripts der kan gennemsøge et site og lave meget brugbare rapporter til dig. Brug nogle timer på Googledorks, og du vil have et meget brugbart billede af hvordan du finder de fortrolige informationer og hvordan du selv undgår at afsløre ting der kan skade dig.

"Select a database to view."
Web-enabled databaser udgør en andet mulighed for hackerne i forbindelse med google. Databasemanagement tools betjener sig ofte af skabeloner til at præsentere dynamiske websider. Hvis du kender disse skabeloner, kan su søge på typiske formuleringer, og dermed finde disse sider direkte. En søgning med "Select a database to view" I Google vil give dig næsten 600 links, hvoraf de fleste vil fører dig direkte til databaser der kan tilgås direkte fra nettet. Alle disse databaser er lavet med FileMaker Pro database interface.
De fleste at disse databaser er relativt harmløse, men enkelte af dem vil indeholde fortrolige oplysninger med bl.a. brugernavne og passwords. Der findes to veldokumenterede sager på nette, den ene hvor Apple Computer havde en database med meget personlige oplysninger på flere hundrede lærere og den anden hvor Drexel University College of Medicine havde lagt en database med 5.500 Neurokirurgiske patienters komplette journaler ud til offentlig tilgang.

Google Cache som hacker værktøj.

De fleste ved sikkert at Google cacher alle de sider den optager i sin database. Dette betyder at selv gamle oplysninger vil være til rådighed for den hacker der kender Googles søgemuligheder og Googles cache funktion. Fortrolige oplysninger, der en gang har været lagt på nettet, risikere altså at være til rådighed for hackerne meget længe. Dette betyder at det er en god ide at gennemtænke hvem i organisationen der publicere informationer på internettet, det skulle gerne være en person der ved vad han/hun gør, og som har en grundlæggende forståelse for sikkerhed og systemsammenhæng. Grundlæggende ligger vores eneste chance for at opdage at hackeren er i gang i de spor hackeren efterlader i vores logfiler. Hvis vi er vågne, og har de rigtige værktøjer til vores rådighed vil vi kunne opdage hackeren allerede mens har er i undersøgelsesfasen. Hackeren har brug for mange informationer før han kan trænge ind og her giver Google's Cache funktion os problemer. Denne funktion giver nemlig hackeren mulighed for at opdage en masse oplysninger uden at sætte spor i vores logfiler og dermed bruge Google til at skjule hvad han har gang i. Løsningen på dette problem er at vi selv bruger Google til at undersøge vores site, så vi fjerner så mange af de farlige informationer som muligt og så vi ved hvilke informationer der trods alt findes på Google. Til det brug kan du anvende Googledorks og så tilføje "site:www.mitsite.dk " til alle søgningerne. Hvis du er heldig, vil du intet finde, og hvis du først analyserer googledorks, kan du også minimere det nødvendige antal søgninger. Om Google faktisk kan bruges til at

skjule iværksættelsen af angreb har jeg ikke fundet bevis for.

Frontpage.
Frontpage, med sin funktionalitet, der på samme tid er let at bruge og svær at gennemskue betyder at mange får publiceret alt for meget. Prøv f.eks. at søge med vti_pvt password intitle:index.of", lidt tålmodighed skulle kunne afsløre ting der kan få det løbe koldt ned af ryggen på enhver der interessere sig for sikkerhed. Hvis du bruger FrontPage, eller et af de andre gode WYSIWYG web editorer, så hold øje med, hvad du faktisk publicere på nettet, brug e.v.t. et ftp program til at uploade med, og vær så opmærksom på hvad du faktisk uploader.

Peer-to-Peer.
P2P her intet med Google at gøre, men da problematikken er den samme har jeg valgt at tage emnet med her. Problemet er selvfølgelig, at folk ikke tænker sig om, og får delt alt for meget ud. Tilsyneladende bruger nogle af P2P tjenesterne at jo mere du deler ud, jo mere får du også selv ud af tjenesten. Dette får nogle til, fuldstændigt ukritisk, at uddele hele deres harddisk. Hvis du kender navnene på de filer der indeholder kritiske oplysninger som brugernavne og passwords, konto oplysninger og andet, vil en søgning med de mest populære P2P programmer give dig alt hvad du behøver til at overtage kontrollen med adskillelige maskiner. Bruger du P2P, SÅ TÆNK DIG OM

Hvad bør jeg gøre for at sikre mig.

BRUG HOVED OG TÆNK DIG OM.

Ændre alle default navne. Dette gælder overskrifter, filnavne (både html, asp, php og database filer), mappenavne, tabelnavne (i databasen) title taggen og især brugernavne og passwords.

Undlad at placere fortrolige informationer på en webserver. **Heller ikke midlertidigt**. Husk at selvom du indskriver placeringen af disse informationer i robots.txt, så søgemaskinen ikke indexisere det, så vil hackerne stadig kunne tilgå og især finde, de biblioteker der er indskrevet i robots.txt. og Googles cache funktion tilsikre at de også kan finde din gamle robots.txt.

Tillad ikke directorie listing. Ved at sørge for at din web server ikke viser indholdet af mapperne, når der ikke er en default web page, fjerner du en del muligheder for hackeren. Har du brug for denne funktionalitet, vær da meget opmærksom på de filer der ligger i ALLE dine web mapper. Og placer ALDRIG filer her midlertidigt, du ikke vil finde igen i f.eks. Google's cache.

Tænk som en Hacker. Hvis du tænker som en hacker, og gennemprøver de værktøjer der findes på dig selv, kan du måske finde nogle huller og uheldigheder der vil kunne udnyttes. Den gamle tese om at "det kræver en tyv for at fange en tyv" er nogenlunde holdbar i denne sammenhæng.

Hack ALDRIG andre ikke engang for sjov, eller for at hjælpe dem med deres sikkerhed. For det første er det strafbart at hacke, og for det andet vil du opdage at folk oftest ikke bliver lykkelige over at du udstiller deres utilstrækkelighed. Du risikere meget let at din hjælpsomhed belønnes med en politianmeldelse og du har under alle omstændigheder et forklaringsproblem. LAD VÆRE, dygtigere folk end dig har fået ødelagt deres fremtid.

Skulle du have spørgsmål, kommentarer eller rettelsen (herunder især stavefejl) er du velkommen til at kontakte mig på kim@bufferzone.dk, ligesom jeg ofte er at finde på Eksperten.

Kommentar af chris d. 15. Mar 2004 | 1

Kommentar af nanoq d. 14. Mar 2004 | 2

Jeg påstår selv, at jeg har ganske godt styr på sikkerhed. Men her lærte jeg alligevel noget nyt. Herligt! :)

Kommentar af tgl d. 04. Aug 2007 | 3

Kommentar af stig3 d. 14. Mar 2004 | 4

Virkelig god artikel. Kan klart anbefales.

Kommentar af jps6kb d. 23. Mar 2004 | 5

Rigtig godt. Fandt selv lidt... *flovt*

Kommentar af thojo d. 27. May 2004 | 6

Super fed :D

Kommentar af 12tri d. 14. Mar 2004 | 7

Kommentar af elf d. 16. Mar 2004 | 8

Kommentar af jensgram d. 08. Jun 2004 | 9

Kan absolut anbefales!

Kommentar af spt d. 14. Mar 2004 | 10

fin artikel... men laver du ikke selv noget ulovligt for at komme frem til din pointe...

Kommentar af skywalker1 d. 23. Jul 2004 | 11

Helt kanon. Velskrevet, gode eksempler, ganske få stavefejl ;-)

Kommentar af tkmbh d. 16. Mar 2004 | 12

Fed artikel. Virkelig spændende.

Kommentar af boomshanka d. 13. Jun 2004 | 13

Nøøøøøøj... :-p

Kommentar af kepsus d. 10. May 2004 | 14

Kommentar af peter_e d. 05. Jan 2005 | 15

Interessant og godt skrevet!! Tak Bufferzone :)

Kommentar af haunted d. 18. Apr 2005 | 16

Kommentar af kometh d. 02. Jun 2004 | 17

Spændende læsning. Godt at vide at der findes kloge danske hoveder indenfor emnet.

Kommentar af nozio d. 15. Jun 2004 | 18

Jeps - Google kan sku' godt være lidt 'uhyggelig' i den forbindelse.

Prøv f.eks. : admin filetype:mdb

Kommentar af cf560 d. 09. May 2004 | 19

Kommentar af j_jorgensen d. 15. Mar 2004 | 20

Tjaa...en oversættelse af artiklen fra Securityfocus.org (http://securityfocus.org/columnists/224) er vel altid godt til dem der ikke kan engelsk. Men de burde istedet følge med hos CERT & Securityfocus.org generelt..samt huske at patche deres software. Brugen af htaccess filer burde måske være nævnt.

Kommentar af blyno d. 17. Mar 2004 | 21

Interessant artikel - ser frem til follow-up's..

Kommentar af waite d. 01. Jun 2004 | 22

Kommentar af moviez d. 17. Mar 2004 | 23

Der er en bog lign. til det "Google Hacker best friend"

Kommentar af mindless d. 15. Mar 2004 | 24

En artikel mange burde læse!

Kommentar af superanden d. 15. Mar 2004 | 25

God artikkel .. dog skriver du at google er en søgemaskine.. For at være helt konkret er det faktisk en søgerobot... yahoo, jubii, kvasir osv er søgemaskiner .. !

Kommentar af anderslarsen d. 18. May 2004 | 26

Rigtig god artikel, dog lidt skræmmende alligevel..

Kommentar af bjanko d. 17. Mar 2004 | 27

Kommentar af doctor6000 d. 28. May 2004 | 28

Kommentar af cyberz d. 03. Jun 2004 | 29

Det er længe siden jeg har læst mig igennem så meget tekst uden at kede mig, meget spændene! Lad os få noget mere af det :-) Et par tips til evt at lukke huller i Apache og ISS kunne være godt, men også for meget at forlange ;-)

Kommentar af wilweb d. 23. May 2004 | 30

Rigtig god artikel:>

Kommentar af eschultz d. 27. Jul 2006 | 31

Kommentar af zarthax d. 08. Jun 2004 | 32

Man kan kun blive klogere for hvert sekund der går :)

Kommentar af morten_leth d. 02. Apr 2004 | 33

kan ikke sige andet end, det er sgu en god artikel, man må jo sige det ikke lige umiddelbart der man kigger først, for at finde ud af sådan noget... ;-) god og velformuleret artikel, thumps up herfra...

Kommentar af ducks d. 21. May 2004 | 34

Glimragende som altid

Kommentar af doktoren d. 15. Jun 2004 | 35

Stof til eftertanke for alle .. Mere af samme skuffe tak :)

Kommentar af phatlasse (nedlagt brugerprofil) d. 17. Mar 2004 | 36

rent guf for øjnene....

Kommentar af cronck d. 17. Jan 2005 | 37

Overraskende

Kommentar af stoltenborg d. 05. Aug 2004 | 38

Er ganske god, når man nu både har egen www server OG bruger google....

Kommentar af hejhej (nedlagt brugerprofil) d. 14. Mar 2004 | 39

God artikel :o)

Kommentar af websafe d. 16. Mar 2004 | 40

Kommentar af rdc d. 15. Mar 2004 | 41

Kommentar af psykerz d. 02. Jul 2004 | 42

Kommentar af humax d. 17. Aug 2004 | 43

Kommentar af ellegaarddk d. 13. Jun 2004 | 44

Kommentar af webcreator d. 24. Apr 2005 | 45

Tak for en god artikel i den velkendte kvalitet fra din side

Kommentar af xozzi d. 10. Jun 2004 | 46

Syyyyg! ikke for børn ;D

Kommentar af verden d. 09. Aug 2004 | 47

Kommentar af ldrada d. 16. Jun 2004 | 48

Meget god artikel.

Kommentar af 477 d. 28. May 2004 | 49

Kommentar af googolplex d. 18. Mar 2004 | 50

Kommentar af jih d. 14. Jul 2008 | 51

Kommentar af snokey d. 05. Feb 2005 | 52

Kommentar af submann d. 21. May 2005 | 53

Kommentar af henrikgn d. 16. Mar 2004 | 54

Kommentar af 911help (nedlagt brugerprofil) d. 14. Mar 2004 | 55

God artikel... :-)

Kommentar af 0nyx d. 20. Sep 2004 | 56

Stavefejl er gratis.. Men har søgemaskiner ikke altid været et alternativ eller..?

Kommentar af los_111 d. 02. Jun 2004 | 57

Rigtigt flot skrevet artikel.
Meget oplysende og spændende på samme tid =)

Kommentar af running_fast d. 14. Mar 2004 | 58

Spændene læsning

Kommentar af sweet-hitman d. 15. Mar 2004 | 59

Artiklen fortæller meget om hacking og at man ikke kan føle sig sikker

Kommentar af tiedt d. 14. Mar 2004 | 60

Kommentar af franck1706 d. 18. Dec 2005 | 61

Kommentar af fcknet d. 16. Jun 2004 | 62

Kanon artikel!

Kommentar af robbin d. 01. Jun 2004 | 63

utrolig velskrevet dog kan jeg ikke erklære mig 100 % enig

Kommentar af tobias28 d. 14. Mar 2004 | 64

Flot!

Kommentar af baronbadedyr d. 07. Jun 2004 | 65

Både lærerigt og underholdende ;)

Kommentar af htmlkongen d. 05. Oct 2004 | 66

Så ved jeg det :) God (velformeleret) artikel, og tak for viden :) /Htmlkongen

Kommentar af peter1234 d. 14. Mar 2004 | 67

Nu troede man lige at Google bare var en søgemaskine

Kommentar af nidyahou d. 14. Mar 2004 | 68

Artiklen giver et godt indblik i hvordan man sikrer sin side mod uønskede gæster. Glimrende gennemgang af søgemaskinens funktionalitet.

Kommentar af kixdreng d. 26. Apr 2005 | 69

sweet

Kommentar af haute d. 01. Jun 2004 | 70

Utrolig skræmmende, jeg må hellere lige rydde op på min hjemmeside, og tjekke for "løse ender" :D Man ved aldrig - det er sket før, og hvordan, ja det ved jeg ikke :S

Kommentar af zaicrez d. 01. Jun 2005 | 71

God Artikel!

Kommentar af christoffero d. 29. Sep 2005 | 72

Fede artikel! :)

Kommentar af anhansen d. 11. Feb 2005 | 73

Cool artikel - sætter fokus på nogle ting som er værd at tænke over..

Kommentar af maqhem d. 01. Jan 2006 | 74

Sej artikel! Lidt forvirrende visse steder, men ellers helt OK

Kommentar af suxor d. 06. Apr 2004 | 75

j_jorgensen > Jeg vidste jeg havde læst artiklen før :D tak for opfriskningen

Kommentar af mikze d. 19. Feb 2005 | 76

wow

Kommentar af dnx d. 27. Mar 2004 | 77

Spændene !

Kommentar af dextor d. 21. May 2004 | 78

GOD artikel!! :)

Kommentar af .jonez d. 01. Oct 2004 | 79

spændende, måske lidt mange fagudtryk eller osse bare fori det er fredag kl 17:47 og man har knppet et par pilss op

sry fejl

Kommentar af kristianlind d. 16. Mar 2004 | 80

Kommentar af vallemanden d. 22. Jun 2004 | 81

Kommentar af karsberg d. 23. Mar 2004 | 82

god artikel!
_karsberg

Kommentar af cheps d. 21. Mar 2004 | 83

Kommentar af amphetamine d. 05. May 2004 | 84

Artiklen giver et meget godt, og grundigt overblik over hvad forskellige værktøjer kan gøre - f.eks. Google som ofte bliver anset for "bare at være en søgemaskine"
-En yderst fornuftig artikel.

Kommentar af ancillus d. 14. Mar 2004 | 85

Smart! Altså smart på en nøj-det-kommer-jeg-aldrig-til-at-bruge-alligevel...men ikke desto mindre smart!

Kommentar af kimfragedved d. 17. Mar 2004 | 86

Kommentar af 4t d. 09. Sep 2004 | 87

Dygtigt skrevet! Spændende indhold, men også noget "uhyggeligt"!
Mente Meget god :-/

Kommentar af therat d. 22. Apr 2004 | 88

en rigtig god artikel, det er da noget man kan tænke over

Kommentar af wanze d. 22. Jul 2004 | 89

Flot artikel!

Kommentar af harthimmer d. 05. Feb 2005 | 90

Kommentar af rnyboe d. 09. Jun 2004 | 91

Kommentar af sorenbs d. 27. Jun 2004 | 92

Kommentar af celebrity d. 29. Jun 2004 | 93

Godt budskab! "Hack ALDRIG andre."

Kommentar af -unknown- d. 23. Jul 2004 | 94

Kommentar af bennylarsen d. 15. Jan 2005 | 95

meget informativt

Kommentar af appeldorff d. 23. Sep 2004 | 96

omg der kan man bare se.. google virker ellers så harmløs

Kommentar af herkules69 d. 03. Oct 2004 | 97

meget fin Artikel

Kommentar af thomaxz d. 14. Dec 2004 | 98

Kommentar af psycosoft-funware d. 04. Jan 2007 | 99

urtoligt godt skrevet!
men jeg vil lige gøre opmærksom på at hacking har en anden betydning; at hacke en dvd afspiller eller andet til at kunne mere / andet end det oprindelidt var tiltænkt fra producentens side.

der vil det være mere på sin plads at bruge cracking = bryde /skaffe sig uautoriseret adgang til data

:)

Kommentar af maijen d. 04. Feb 2005 | 100

God artikel... Giver stof til eftertanke.

Kommentar af jonathan87 d. 14. Mar 2005 | 101

Interesaant artikel. Godt skrevet(forfatteren har dog nogle problemer med nutids-r)

Kommentar af truzy d. 26. Oct 2005 | 102

Kommentar af nickill d. 28. Dec 2005 | 103

Kommentar af phpzer0 d. 16. Apr 2006 | 104

Kommentar af j4k0b d. 05. Feb 2007 | 105

Kommentar af jp4200 d. 24. Jul 2007 | 106

Kommentar af juliedahl d. 14. Jul 2008 | 107

cool.. selv for en der ikke ved meget om det