COMPUTERWORLD

Hackere - Hvordan arbejder de.

Hackere, hvordan arbejder de, hvad gør de for at komme ind på din PC og hvad kan jeg selv gøre for at opdage dem, når de er på vej. Hvis du ved hvordan din fjende arbejder, ved du også hvordan han skal slåes.

Skrevet den **03. Mar 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Hackere - Hvordan arbejder de.

Denne artikel er gennemset og godkendt af Coadmin, den holder sig inden for ekspertens regelsæt. Det at vide hvordan en hacker arbejder, er ikke det samme som at vide, hvordan man gennemfører hacking. Denne viden er derimod helt nødvendig, for at kunne gennemføre sikker administration af et netværk og af serverer.

Læs også
The Hacking Dojo 1 - Sådan hacker du - Introduktion (http://www.eksperten.dk/artikler/1233)
The Hacking Dojo 2 - Sådan hacker du - Byg dit Lab (http://www.eksperten.dk/artikler/1234)
The Hacking Dojo 3 - Sådan hacker du - Sniff bare, det lugter ikke (http://www.eksperten.dk/artikler/1245)
The Hacking Dojo 4 - Sådan hacker du - Så går vi aktivt (http://www.eksperten.dk/artikler/1251)

Religion eller???

Vi er lige nødt til først at formulere os ud af en religionskrig, der ikke er relevant her. Jeg kender den oprindelige betydning af ordene hacker og cracker. Diskussionen om hvad det kaldes, og hvad der er den rigtige betegnelse, er der nogle der går meget op i. For mig er det fuldstændig lige meget hvad vi kalder det, bare vi ved hvad vi taler om. I denne artikel bruger jeg den almindeligt anerkendte betydning af ordet "Hacker", der defineres som en person, der bryder ind i netværk med onde eller andre hensigter. Folk der ønsker at diskutere om det ikke bør hedde en cracker, er meget velkommen til det, forvent dog ikke at jeg deltager.

Når du nu læser om hvordan en hacker arbejder er der selvfølgelig tale om generelle betragtninger, idet hver enkelt hacker naturligvis har sin egen måde at gribe tingene an på, og sikkert også kan finde på at variere metoden. Artiklen beskriver de faser, der kan gennemgås af en hacker.

1. Angrebet startes, målet identificeres.
Du kan blive mål for en hacker på mange måder. Forskellige hackere identificerer deres mål på forskellige måder og mål kan også identificeres ud fra, hvad det er hackeren ønsker at gøre.
Nogle gange vil du blive fundet ved en tilfældighed. En hacker kan iværksætte en gennemscanning af en mere eller mindre tilfældig valgt gruppe af IP adresser, for at identificere, om der er nogle af disse adresser der skulle indeholder en computer med nogle interessante porte åbne, eller andet der kunne indikere, at her er der en computer det kan betale sig at kikke på. Denne tilfældige metode anvendes rimeligt ofte af alle slags hackere, professionelle som de rene amatør. Amatørerne fordi de ikke ved bedre, de professionelle fordi de har brug for mange computere, bl.a. til at skjule sig bag ved.

Den seneste tid har Mohammed sagen, har tydeligt vist at man kan blive et mål på mange forskellige

måder, herunder blot fordi man er dansk, muslim eller på anden måde tilhørende en eller anden gruppering

Du kan også blive udvalgt fordi du på den ene eller anden måde er synlig. Du kan f.eks. findes via ICQ, Messenger, på Skype, i nyhedsgrupper, på fora (ja også på eksperten) og alle andre steder hvor du stikker næsen frem. Hvis du afslører dig selv som en ren amatør, kan du være interessant fordi du så er relativt lettere at hacke, og hvis du afslører dig selv som dygtig kan du være interessant fordi du er en udfordring. Vær den grå anonyme mand/kvinde det er sikrest. Hvis du har forskellige servere kørende på nettet, f.eks. en web server eller en mailserver, vil du være dobbelt synlig, dels fordi en server skal være synlig, og dels fordi disse, samt ftp serveren, giver en hacker en masse dejlige muligheder, der gør dig meget mere interessant.

2. Rekognoscering. Kend dit mål
Det første en hacker vil gøre er normalt en portscanning, for at se hvilke porte der er åbne på din maskine. Portscanningen kan foretages på et væld af forskellige måder. Nogle af disse måder er meget lette at genkende i din logfil og vil blive opdaget af alle Intrusion Detection systemer (IDS), andre metoder er næsten umulige at opdage. En professionel hacker, vil gennemføre sin portscanning over lang tid, fra mange forskellige computere og han vil måske ikke scanne alle porte. En sådan portscanning opdager du ikke ved at kigge i din log, og IDS har heller ikke en chance. Den professionelle hacker vil altid validere sin portscanning manuelt, for at se om de porte der er fundet virkelig er åbne, og om muligt hvad der er bag dem. Denne validering vil ofte anvende helt almindelige teknikker, der er lovlige og ikke vil se mistænkelige ud i loggen. F.eks. kan port 80 valideres ved at prøve at åbne websiden i en browser. Da det er præcis det en webserver er beregnet til, vil du ikke bemærke at en tilfældig bruger har været inde på dit website, dem er der jo mange af hver dag.

Trin nummer to vil være en sårbarhedsscanning med forskellige sårbarhedsscannere. Denne scanning kan foretages efter de samme principper som portscanninger, alt efter hvilket værktøj han vælger. Nogle værktøjer kan konfigureres mere en andre, nogle værktøjer er bedre til at skjule deres scanninger end andre. Er der tale om en professionel hacker, vil du kun med held og hårdt arbejde kunne se, at der er noget i gang i din logfil, og IDS har heller ikke en chance. Det du skal kigge efter i din logfil er mærkelige entries, f.eks. en URL forespørgsel med rigtig mange A'er eller andre tegnkombinationer. Dette kan indikere en sårbarhedsscanning eller en orm der forsøger at komme ind.
En sårbarhedsscanning vil af den professionelle hacker altid blive efterfulgt af en manuel validering af de fundne sårbarheder. De gode sårbarhedsscannere kan foretage det der kaldes en sikker scanning. Flere af sårbarhederne er så kaldte Denial Of Service (DOS) sårbarheder, altså sårbarheder der vil få din maskine til at gå ned. Hvis en scanner gennemprøver en sådan sårbarhed for at teste om den findes, vil din maskine jo gå ned, hvorefter der ikke kan testes for flere sårbarheder. Derfor vil de gode sårbarhedsscannere kun sandsynliggøre at sårbarheden eksistere. Den manuelle validering skal vise om den faktisk er der.
Analyse af web-serveren, indeholder både scanning med sårlige sårbarhedsscannere for web-servere, samt manuel gennemgang af koderne. Mange anvender færdige løsninger downloaded fra nettet, det kunne f.eks. være Snitz forum, PHPBB, eller en købeløsning fra et firma. Disse løsninger indeholder selvfølgelig også huller og sårbarheder der kan anvendes. En af de mest almindelige sårbarheder er mulighed for SQL injektion, hvor en hacker relativt let kan skaffe sig administrator login oplysninger. Hvis administratoren så har været doven og anvendt det samme password som han anvender på systemet (mennesket er jo dovent af natur) så er der fri adgang på alle hylder.
Endelig findes et væld af forskellige scannere, der anvender forskellige teknoligier til at finde ud af hvordan computeren eller netværket hænger sammen. Dette kunne f.eks. være Firewalk der anvender Tracrout og andre afsamme slags.

3. Planen.
Efter portscanningen, sårbarhedsanalysen og især de manuelle valideringer vil hackeren, hvis han bare har lidt fat i, hvad det er han gør, have et fuldstændigt billede af hvad det er han sidder over for. Hvilket

styresystem der er installeret f.eks. Windows 2000 server, hvilken servicepack der er installeret, hvad der ellers er installeret af vigtige programmer, hvilke brugere der findes på systemer, hvilke ressourcer der er delt ud og e.v.t. hvilke andre brugere der er oprettet i web systemerne. Derudover vil han nu have en liste over sårbarheder der kan udnyttes samt vide hvordan de forskellige sårbarheder udnyttes.
Planen kan nu lægges, hvilken sårbarhed vil han værke, hvad vil han opnå på dit system, hvilke værktøjer får han brug for.

4. Angrebet startes.
Hackeren vil normalt vælge tidspunktet med omhu. Han vil vælge et tidspunkt hvor der er lille sandsynlighed for at du sidder foran serveren. Hvis han anvender en sårbarhed der også får serveren til at gå ned (DOS) vil han vælge et tidspunkt hvor der ikke er mange brugere på. Omvendt vil han vælge et tidspunkt hvor der er mange på hvis sårbarheden ikke får serveren til at gå ned, og på den måde forsøge at skjule de entries der vil komme i din log blandt mange andre lovlige entries.
Angrebet startes med at en exploit køres af, enten en exploit der er downloadet fra nettet, eller en exploit hackeren selv har skrevet. I næste fase henter hackeren sine værktøjer op på serveren, og bruger disse til at skaffe sig administrator rettigheder. Ofte vil exploiten skaffe ham system rettigheder. Disse muliggør at han kan hente password filen, der så kan crackes på hans egen maskine. Hvis du har brugt et dårligt password (der kommer en artikel om passwords senere) kan administrator passwordet crackes på ganske få sekunder til et par timer, hvorefter han anvender et værktøj til at hæve rettighederne fra system til administrator, og han er nu inde og kan gøre hvad han vil. Faktisk findes i dag værktøjer, der stort set automatiserer hele processen.

5. Vildledning.
Når han nu er inde på dit system, vil det næste han gør, være at forsøge at slette sine spor. Først vil han redigere eller slette din logfil, så sporene efter ham der er væk.
Herefter vil han skjule sine værktøjer. Dette kan gøres på forskellige måder, med og uden værktøj, den ene metode kan du selv prøve.

Metode 1: Rootkit
Et rootkit er et farligt stykke værktøj, der aldrig burde være opfundet. Rootkittet skjuler alt hvad hackeren gør og placerer på din server. Han kan oprette biblioteker, han kan placere filer og han kan oprette brugere, og du vil aldrig kunne se disse ting med de værktøjer og programmer du har til din rådighed som administrator. Hvis du ikke har haft et hostbased IDS på dit system, vil du aldrig kunne opdage, at der er en hacker på dit system, han er helt skjult for dig, og eneste løsning er en formatering og komplet re-installation af dit system. Husk at det faktisk ikke er nok at re-installere, han kom jo ind første gang, og vil komme ind igen hvis du ikke gør noget andet og mere end du gjorde sidste gang. Skift alle password til stærke passwords, installer et hostbased IDS, trim din server op.

Metode 2: Udnyttelse af NTFS stilængde begrænsnings sårbarhed.
NTFS filsystemet har en sårbarhed eller facilitet, alt efter hvordan du ser på det. En NTFS sti kan max være 256 karakterer lang i Windows, men i praksis kan den være længere, Windows kan bare ikke håndtere den. Prøv at starte på dit C:/ drev med at lave et bibliotek der hedder 123456789, herefter går du ind i dette bibliotek og laver et bibliotek med samme navn, herefter går du ind i dette bibliotk og laver et bibliotek af samme navn. Dette bliver du ved med indtil Windows fortæller dig at du ikke kunne oprette biblioteket. Du er nu stødt på de 256 karakterers loft, og du har en sti der ser således ud: C:/123456789/123456789/123456789/123456789/...../123456789/. For at kunne lave yderligere biblioteker der er skjult, må du nu snyde systemet til at tro at stien ikke er så lang, det gør du ved at substituere den lange sti med et drev bogstav. Du kan gøre det i windows eller med dos kommandoen Subst således: subst f: C:/123456789/123456789/123456789/123456789/...../123456789/ Du kan nu åbne dit nye f:/ drev og lave yderligere et par biblioteker og placere nogle filer herinde. Når du nu fjerner det mappede drev (f:/) og forsøger at tilgå de filer du har placeret i det yderste bibliotek gennem c:/123456789/ osv osv, vil du ikke kunne få lov, heller ikke selvom du er administrator. Eneste måde at få fat i de yderste biblioteker på, er at substituere stien med et netværksdrev igen og så gå ind den vej.

Det sidste hackeren vil gøre, hvis han er rigtig god, er at lukke de huller i dit system han har fundet. Du

kan altså være ude for at en hacker installerer servicepacks og sikkerhedsopdateringer på dit system for at lukke hullerne han selv er kommet ind af. Dette gør han selvfølgelig for at forhindre andre hackere i at komme ind op ødelægge tingene for ham.

Hackeren har nu fuld adgang til dit system og mulighed for at gøre som han lyster, hvis han er god, er det eneste du nu kan gøre at formatere din maskine.

sikre sig adgang.
Når hackeren har opnået fuld adgang til dit system, vil han sikre sig at han beholder denne adgang. Dette sker dels gennem installation af alternative bagdøre og gennem forsøg på kompromittering af andre maskiner i dit net (hvis der er nogle). Du vil kunne forvente at en ahcker vil forsøge at få kontrol med så mange maskiner som muligt og hvis han er god, vil han installere forskellige værktøjer på de forskellige maskiner, for at sikre at der altid er mindst et værktøj der ikke er blevet opdaget.
Har du haft besøg i dit netværk og er du ikke i stand til fuldstændigt at dokumentere hvor han har været, kan du risikere at eneste løsning er en total formatering af alle enheder på dit net efterfuldt af reinstallation fra sikre medier.

Du er selvfølgelig velkommen til at stille spørgsmål her på eksperten, samt at kontakte mig på kim@bufferzone.dk for yderligere spørgsmål. Kommentarer og forslag samt rettelser af stavefejl modtages med kyshånd.

Kommentar af steen d. 14. Jan 2004 | 1

Kommentar af simonvalter d. 15. Jan 2004 | 2

udemærket, som du selv siger er der selvfølgelig mange andre fremgangsmåder som hackere benytter sig af afhængigt af hvilken type de er og hvad de vil opnå, men det er jo også begrænset hvor meget man kan dække i en enkelt artikel.

Kommentar af nse d. 16. Jan 2004 | 3

Bestemt en god og velformuleret artikel der kort beskriver en hackers fremgangsmåder... Meget god

Kommentar af jones d. 01. Dec 2004 | 4

Rigtig god !!!

Kommentar af hermandsen d. 22. Jan 2004 | 5

Spændende artikel! Helt sikkert den sjat point værd! :)

Kommentar af karsten_larsen d. 27. Jan 2004 | 6

Interessant artikel.

Kommentar af tumlehund d. 01. Dec 2004 | 7

Spændende.

Kommentar af jakobgt d. 26. May 2005 | 8

Ganske god. Man kan ikke lade være med at få respekt for en hacker, når personen gør så meget ud af det.

Kommentar af j_jorgensen d. 31. Mar 2005 | 9

Udemærket artikel som beskriver en ekstern hackers muligheder for at bryde ind.

Kommentar af lomse d. 21. Jan 2004 | 10

God artikel, man bliver helt bange for at blive deres næste offer.

Kommentar af athlon-pascal d. 15. Jan 2004 | 11

En kvalitetsartikel - Alle pointene værd! :o)

Kommentar af ducks d. 17. Jan 2004 | 12

Håber du kommer til at skrive maaange artikler herinde :-)

Kommentar af blackadder d. 21. Jun 2004 | 13

En af de bedre artikler. Interessent læsning.

Kommentar af hejhej (nedlagt brugerprofil) d. 15. Jan 2004 | 14

God artikel :-)

Kommentar af _michael_ d. 22. Jan 2004 | 15

Kommentar af elmoe d. 26. Aug 2004 | 16

Du ved sgu hvad du taler om!

Kommentar af punnishment d. 28. Nov 2004 | 17

Sü'per!

Kommentar af rdc d. 31. Jan 2004 | 18

Spændende og god artikel.

Kommentar af eagle124 d. 17. Jan 2004 | 19

fantastisk artikel du har fået lavet der

Kommentar af ldrada d. 15. Jan 2004 | 20

Udemærket.

Kommentar af desi-mus d. 23. Feb 2004 | 21

Kommentar af sir_plexus d. 19. Feb 2006 | 22

Giver god basis viden om hvordan hackere arbejder og hvad deres hensigt kan være! Meget god artikel!

Kommentar af deadmez d. 29. Nov 2004 | 23

Hmmmm... nu ved vi jo hvordan det gøres.... øøh... eller noed... ej... skal nok være sød.. *GG*

Kommentar af morty d. 15. Jan 2004 | 24

Kanon artikel...

Kommentar af googolplex d. 16. Jan 2004 | 25

Fin artikel :)

Kommentar af robbin d. 31. Aug 2004 | 26

meget flot genemgang

Kommentar af htmlkongen d. 29. Nov 2004 | 27

Som sædvanlig: Perfekt :)

Kommentar af ttj d. 24. Aug 2004 | 28

God og spændende artikel!

Kommentar af cd4all d. 21. Feb 2006 | 29

interessant

Kommentar af rasmusbl d. 21. Feb 2006 | 30

Kommentar af kjerum d. 03. Jun 2005 | 31

Utrolig fangende læsestof, man bliver sindssygt opslugt...

Kommentar af the_ghost d. 20. May 2005 | 32

Rigtig god artikel. devilinheaven >> Som han skriver i starten behøver en administrator ikke have kendskab til hacking, men kendskab til den måde en hacker arbejder på. - Der er stor forskel.

Kommentar af jonat d. 02. Sep 2004 | 33

Godt arbejde (igen) ;).. keep up the good work :D

Kommentar af neo2k d. 28. Jul 2004 | 34

God artikkel, godt skrevet. Relevant og informativ.

Kommentar af syntax_hh d. 15. Jan 2004 | 35

Laaaang artikel, og meget god :)

Kommentar af fauer d. 25. Jun 2004 | 36

Tak for god og relevant information.

Kommentar af jorgena d. 27. Feb 2006 | 37

Spændende læsning!

Kommentar af sorenbs d. 24. Nov 2004 | 38

Giver et godt og hurtigt indblik i hvad man skal være opmærksom på. På en gang skræmmende og faschinerende :)

Kommentar af mantichora d. 07. Oct 2005 | 39

sehr gut mein herr.

Kommentar af trophymanager d. 25. Aug 2005 | 40

Argh. Jeg tror jeg bare slukker min egen webserver nu og køber noget hosting et sted :)

Kommentar af devilinheaven d. 04. Feb 2005 | 41

du mener man skal have kendskab til hacking for at være adminstrator og alt muligt pis..... Du må ikke engang hacke din egen server hvis du har sådan en og din kode er glemt eller noget.... så ryger du sku ind selvom det var fordi du ikke kunne huske din kode... så det behøver man ikke at have kendskab til... jeg synes det er åndsvagt at hacke... synes du ikke...

Kommentar af teefax d. 24. Aug 2004 | 42

Skræmmende...! Men god artikel, og gode oplysninger som man sjældent finder!

Kommentar af ranglen d. 16. May 2005 | 43

Kommentar af myg0th4x d. 29. Aug 2004 | 44

lol ;)

Kommentar af rowdy d. 31. Aug 2004 | 45

Selvom, man ikke lige er ekspert på det område, så siger det en del!

Kommentar af lunanol d. 25. Dec 2004 | 46

Meget oplysende...

Kommentar af superwulff d. 27. May 2005 | 47

det er sgu en dejlig artikel. som jakobgt skrev. Man kan ikke lade være med at få respekt for en hacker... Keep up the good work!

Kommentar af areon d. 25. Nov 2004 | 48

10 pil opad for en informativ, læsevenlig og SPÆNDENDE artikel. ser frem til at læse det næste du kommer ud med.. :=)

Kommentar af mtj111 d. 20. May 2005 | 49

Nice artikel :-) Glæder mig til artiklen om passwords kommer!

Kommentar af ziox d. 25. May 2005 | 50

Hva' med en hacker guide? ;) :D Rigtig god artikle, kunne godt tænke mig at lære at hacke, roder selv meget med mIRC, fx. auth-hacking, proxyclones og overtake.

Kommentar af sjollermand d. 25. Feb 2005 | 51

Rigtig go Artikel

Kommentar af djio d. 03. Jun 2005 | 52

Super! Har læst et par historier og sådan, men denne var dog den bedste! =)
Keep up the good work =]

Kommentar af joejjoej d. 27. Nov 2005 | 53

Kommentar af permie d. 15. Sep 2005 | 54

Kommentar af monkeylover d. 09. Mar 2006 | 55

Den er super.. giver et kanon indblik i hvordan hackeren arbejder! GJ! :P

Kommentar af lassemelbye d. 07. Sep 2006 | 56

Meget godt at vide!

Kommentar af mcmini d. 05. May 2006 | 57

Syns den giver et godt overblik så man er forberedt

Kommentar af mygi d. 30. Sep 2006 | 58

nice

Kommentar af egzonrh d. 22. May 2008 | 59

Nicht slecht. Det er godt at vide hvordan de små rotter snuser rundt i vores computer.