Chill

Hackerguiden 2.013

Hacking - Træk og modtræk

Index

FORORD ---- 8

1. METODER OG TEKNIKKER ---- 11

VIRUSSER OG SPYWARE ---- 12
DET TRÅDLØSE NETVÆRKS HURTIGE UDVIKLING ---- 13
KENDTE EKSEMPLER ---- 14
ANALYSE AF ET TYPISK ANGREB ---- 16
FORBEREDELSE AF ET ANGREB ---- 17
ONLINE ---- 18
LEG OG LÆR ---- 18

2. TCP/IPS SVAGHEDER ---- 21

LIDT HISTORIE ---- 21
HVAD SÅ I DAG? ---- 23
TCP/IP: RODEN TIL ALT ONDT? ---- 23
ET LIDT FOR OFFENTLIGT NETVÆRK ---- 24
STANDARDEN TCP/IP – PROGRAMMERNES SVAGE PUNKT ---- 27
MATERIEL OG HULLER ---- 28
SNIFFING ---- 29
TEST DIT NETVÆRK MED WINPCAP OG LIGNENDE ---- 29
ICMP OG PROGRAMMERNE NETSTAT OG ROUTE ---- 34
AT HIJACKE ROUTEN ---- 36
MODTRÆK ---- 38
I DAG IPV6 ---- 39
TYPE 0 ROUTING HEADERS ---- 39
SMUT FORBI ---- 40
FEJLKONFIGURERING ---- 40
UNDERSTØTTELSE ---- 40
PRÆSTATION ---- 40

3. HACKERVÆRKTØJER ---- 41

KENDE NETVÆRKET ---- 41
PING OG TRACEROUTE ---- 41
ANDRE VÆRKTØJER ---- 43
SCANNERE ---- 45
IDENTIFIKATION AF SYSTEMET ---- 45
SCANNING KAN VÆRE FARLIGT ---- 47
MODTRÆK ---- 49

4. SPYWARE, VIRUSSER OG TROJANSKE HESTE ---- 51

TROJANSKE HESTE ---- 51
BESKRIVELSE AF EN TROJANSK HEST ---- 51
DARKCOMET: STJERNEN … ---- 53
HVORDAN TROJANSKE HESTE BLIVER INSTALLERET ---- 54
LIDT PRAKTIK ---- 56
VIRUSSEN ---- 60
MAKRO-VIRUS ---- 61
DEN MODERNE TROJANSKE HEST: SPYWARE ---- 62
ANTIVIRUS, ANTITROJANSKE HESTE OG ANTISPYWARE ---- 63
FALSK ALARM ---- 63

DIN PUTER OPFØRER SIG ÅNDSSVAGT ---- 64
NÅR DER ER VIRUSSER TIL STEDE ... ---- 65
SKIL DIG AF MED TROJANSKE HESTE ---- 66
FIND OG SLET SPYWARE ---- 67
EN VERDEN UDEN VIRUSSER? ---- 68

5. SYSTEMHULLER ---- 69

ANALYSER RESULTATET AF EN SCANNING ---- 69
EXPLOITS ---- 70
MAILING-LISTERNE ---- 71
VÆRE MORSOM MED DEFACING ---- 71
HULSCANNEREN ---- 73

6. INTERNET-PASSWORDS ---- 75

OMGÅ PASSWORDS ---- 76
SOCIAL ENGINEERING VS. BRUTE FORCE ---- 77
PASSWORDGENERATORER ---- 77
TEKNOLOGI OG STATISTIK VS. PASSWORDS ---- 79
ANGREB MED PASSWORDS ---- 80
SIMULER EN BRUGER ---- 81
BRUTUS' BRUTE FORCE ---- 82
BRUTUS' MULIGHEDER ---- 84
ANGREB MOD EN HTML-FORMULAR ---- 85
MODTRÆK ---- 86

7. PC-PASSWORDS ---- 89

PASSWORDKATEGORIER ---- 89
BIOS-PASSWORD ---- 90
AFBRYD ALT! ---- 90
EN TROJANSK HEST I DIN PC ---- 91
SYSTEMPASSWORDS ---- 91
WINDOWS-PASSWORDS ---- 91
CRACKERS, SOM BRUGER DIN MASKINE ---- 93
WINDOWS- OG LINUX-PASSWORDS ---- 93
MODTRÆK ---- 97
OFFICEPAKKER ---- 98
MODTRÆK ---- 98

8. BESKYT DINE DATA ---- 99

BESKYT DIG ... MEN IKKE FOR MEGET! ---- 99
RSA ---- 99
GNUPGP I PRAKSIS ---- 101
MODTRÆK TIL PGP: TASTATUR-SNUSERI! ---- 103
MODTRÆK? ---- 104
STEGANOGRAFIEN, HVAD ER DET? HAR DEN FORDELE? ---- 105
STEGANOGRAFIEN I DAG ---- 106
STEGANOGRAFI-PROGRAMMER ---- 107
INVISIBLE SECRETS ---- 107
SECURENGINE ---- 108
LIDT PRAKSIS ---- 108

9. SKJULE SINE SPOR ---- 115

KAMUFLERINGSTEKNIKKER ----115
WIRELESS NETVÆRK OG WARDRIVING ----116
BRUGEN AF FALSKE IP-ADRESSER ----117
OFFENTLIGE PROXIES ----117
ANONYME PROGRAMMER ----118
TOR ---- 118
STEALTHY ---- 119
I GANG MED TOR ----119
NU SKAL DU OGSÅ LIGE ... ----123

10. SOCIAL ENGINEERING ----125

GIV MIG ----126
JEG GIVER ----128
MYNDIGHED ----129
ESSENSEN ----131

HACKING ER SJOVT ----133

Forord

"En pirat er først og fremmest en, som forsøger at lave en uautoriseret handling på netværket, på sit "mål"... Altså du, som privatperson eller kommende administrator af en eller flere computere: Du er hans mål. Den bedste måde at beskytte dig imod et angreb på er at forstå, hvordan piraten vil handle, og bruge de samme værktøjer som han."

Sådan skriver Chill i bogen her.

Jeg vil spille djævelens advokat og skære den rystende sandhed endnu mere ud i pap for dig.

Forestil dig, at du lever i en verden, hvor alle mulige slags avanceret indbrudsværktøj ligger frit tilgængeligt rundt om i butikkerne, på gaderne og i andre folks hjem.

Forestil dig ligeledes, at du er en ganske almindelig husmor eller -far, og du har lært, at du skal låse døren, når du går hjemmefra. Vil denne beskyttelse hjælpe dig? Nej, ikke spor, for de værktøjer, som ellers er forbeholdt låsesmede, kan findes af enhver 12-årig dreng, og i løbet af få sekunder kan han skaffe sig adgang til dit hus.

Du troede ellers, at det var godt nok at låse, fordi du troede, at man skulle have en nøgle for at låse op igen. Din uvidenhed gjorde dig til offer.

Chill er her for at fortælle dig, hvordan indbrudsværktøjerne fungerer. Ikke så du selv skal begå indbrud, men så du ved, hvordan du bedst beskytter dig imod det eller i hvert fald gør det så besværligt for indbrudstyven, at han vil foretrække at gå til det næste hus i stedet.

For på nettet ligger disse værktøjer frit tilgængeligt. Din uvidenhed vil ikke beskytte dig, heller ikke selv om du har beskyttet din pc med en adgangskode.

Målgruppen for denne bog er ikke tyvene, men den gode husfar eller -mor. Det er systemadministratoren, det er den almindelige pc-bruger.

Du vil i takt med, at du læser bogen, lære din pc's og internettets svagheder at kende, du vil se på it-piratens værktøjer, du vil afprøve dem på dit eget system, og du vil lære modtrækkene at kende.

Gem denne bog, for du vil slå op i den igen og igen. Sikkerhed er noget, der hele tiden skal vedligeholdes, forbedres og bearbejdes. Du vil glæde dig over at kunne bevare dine data, både på pc'en og internettet, for der er næppe noget værre end at skulle bruge mange timer på at forsøge at genskabe noget, når det kunne have været undgået.

Glem alt om kedelig læsning og unyttig viden. I denne bog får du det sjovt, og du vil komme legende til større sikkerhed på din computer og hjemmeside.

Forfatteren til denne bog går under hacker-navnet Chill. Han startede sin hackermæssige løbebane allerede i 1985, da han netop havde fået sin første computer, en Commodore 64, som gemte data på kassettebånd. Chill havde købt et rigtig godt spil, og da han gerne ville lære, hvordan det var skrevet, hackede han sig ind på det for at se koden. Det var svært, men lykkedes efter nogle ugers stædig kamp. Senere gjaldt det om at komme i kontakt med andre computere på netværket, og Chill skaffede sig adgang til nummeroplysningen. Dog var de hemmelige numre også hemmelige dér.Det er en stor ære for mig som Chills kone at have fået lov at

skrive dette forord. Men nok snak. Jeg vil nu overlade ordet til Chill, som har lidt at fortælle dig om hacking. God fornøjelse!

September 2007, Britt Malka

Opdatering:

Seks år er gået, siden første udgave af Hackerguiden udkom.

Seks år!

Man skulle tro, at der var færre hackerværktøjer til rådighed, nu hvor man efterhånden kender til problemet, ikke?

Man skulle tro, at pc'er var blevet sikrere, og at hjemmesider ikke kunne hackes så nemt.

Desværre er det ikke tilfældet.

Hackerguiden er lige så aktuel i dag, som den var for seks år siden.

Chill har gennemgået hvert eneste kapitel og opdateret den til tidssvarende forhold.

Nu er det din tur. Prøv de dirke, som kan bryde din dør op i dag, og sørg for at lukke hullerne så godt som muligt, så tyvene vælger andre huse i stedet.

Marts 2013, Britt Malka

1. Metoder og teknikker

Oprindeligt havde ordet "hacking" en mystisk og skræmmende klang, og det har det stadigvæk for mange den dag i dag. Dog forstår alle ikke betegnelsen "hacker" på samme måde. Det er afhængigt af, om man er it-nørd og interesseret, eller et muligt offer. Hvilken side står du på? Før vi går i gang med selve emnet, hacking, skal vi lige se på it-pirateringens landskab og de forskellige teknikker og "familier", det deles i. Vi går en lille rundtur og ser på metoder, historien, eksempler og sætter begreber på plads. I denne bog er det princippet, at alle svære eller nye ord vil blive forklaret. Så bare slap af, læn dig tilbage, og læs videre. Du vil få alle de forklaringer, du har brug for.

Før i tiden, dengang computerne gik på gas, var en hacker nødvendigvis en programmør. Der var tale om en rimelig genial person, som var i stand til at gøre hvad som helst med en computer, uanset hvordan den var beskyttet.

Selv om den geniale person stadigvæk eksisterer, så er han som regel ikke årsag til de forskellige angreb, man hører om jævnligt. Han overlader mere og mere pladsen til "*lameren*" (eller script-kiddy). En "lamer" er en nybegynder-pirat, som ikke er på niveau med disse it-eksperter, men som nogenlunde godt kan bruge de forskellige online-værktøjer, man kan finde rundt omkring.

Lad os ikke tage fejl: I denne bog vil vi oftere tale om lamerens teknikker, end vi vil tale om den ægte hackers teknikker. Det er ganske enkelt, fordi sidstnævnte slet ikke bruger andres teknikker, men er en it-nørd på meget højt niveau, meget kreativ, som opfinder nye former for piratering, og som kan udvikle værktøjer ... som vil blive brugt af lameren.

Dagens virkelighed er sådan: Med undtagelse af få imponerende angreb viger den "geniale hacker" pladsen for disse "små-hackere" eller, værre, for lamere som nøjes med at udnytte værktøjer, som er skabt af andre, informationer, som andre har fundet ud af, og dem udnytter de for at lave deres egne angreb og problemer.

Derfor er det i dag nemt for alle via internettet at få fat i stort set et hvilket som helst automatiseret program og den medfølgende brugsanvisning for at lave et angreb. Følgelig kan vi se en stor stigning i antallet af angreb rundt omkring. Her er den metode, sådan en amatør-pirat vil bruge:

- ❑ Han vil nøjes med at identificere et mål med et program (en scanner for det meste, det vil vi snakke om).
- ❑ Han finder ud af, hvilke programmer eller systemer der er installeret på målet.
- ❑ Han finder huller i de programmer, som er installeret, ved at benytte de forskellige brugsanvisninger og dokumenter, der kan findes på nettet.
- ❑ Han downloader et program, som kan udnytte disse huller.
- ❑ Han angriber systemet.

Der er ikke meget svært ved det. En hvilken som helst bruger med lidt kendskab til nettet og til sit system kan gøre det. Den pirat, vi taler om her, har aldrig nogensinde selv skrevet en eneste kodelinje, men kan ramme stort set en hvilken som helst maskine: Windows XP, Vista, Windows 7, Linux, Apache server web m.fl. 99 % af de angreb, der foretages, sker via forudprogrammerede teknikker.

Han har intet at gøre med hackeren, som kender Linux, Windows eller Apache på fingerspidserne, som kan opfinde nyt, tænke det igennem, finde et ukendt hul og teste det ved hjælp af forskellige programmer, som han selv har skrevet i C eller i Assembler. Hackeren, den ægte, vil bruge *Reverse-coding* eller *decompilation* for at forstå programmer, og han ved, hvordan en computers processor arbejder.

Men det er altså lameres angreb, man husker og kender til, og ikke hackerens. Det er lameren, som vil efterlade sig spor, som vil lave en *defacing* af din hjemmeside (ændre forsiden), eller – værre – slette den eller installere et hackingforum på din server.

Du vil sjældent læse om det i nyhederne eller rundt omkring, men ret mange systemansvarlige i store firmaer har lige pludselig fundet ud af, at en pæn del af deres system eller båndbredde bliver brugt af pirater, som udnytter deres server eller internet-forbindelse til at sprede deres informationer eller til at angribe deres system.

> **Reverse-coding (eller decompilation): Metode, som benyttes til at genfinde kildekoden fra et program. Før et program bliver til en .exe-fil, skrives det i et bestemt programmerings-sprog.**
>
> **Decompilation eller reverse-coding går ud på at genfinde det originale program og dermed forstå, hvordan det er blevet programmeret … og finde dets fejl og huller.**

Virusser og spyware

I denne bog vil vi også tale om spyware (spion-programmer) i forbindelse med trojanske heste. Disse to metoder benyttes bredt på nettet, og brugen af spyware stiger støt.

I hele 2012 blev der skabt mellem 3 og 6 millioner nye *malwares.* Tallet svinger, fordi det kommer an på, hvad de forskellige antivirus-firmaer antager for at være malware, og om man medtager smartphones, tabletter m.m. eller ej. Af disse var 80 % af malwaren på nettet trojanske heste i forskellige former.

> **Malware: Malware er en sammentrækning af de engelske ord MALicious softWARE (egentligt "ondsindet program"). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på. Virusser, spyware, dialere m.m. er malware.**

Den store stigning skyldes, at spyware ikke kun benyttes af pirater, men også af forskellige firmaer, der sælger deres varer via spyware.

Spyware er ikke så metodisk som hacking. Det er en slags hybrid mellem virussen og den trojanske hest og er helt automatisk: Det kommer ind i din maskine og forsøger at få fat i dine koder eller studerer dine vaner, udskifter reklamer på den side, du besøger m.m.

Formålet med metoden er enten kriminelt eller business.

Det trådløse netværks hurtige udvikling

Siden 2001 har det trådløse netværk opnået stor fremgang, og systemet bruges ofte af pirater, så de kan surfe gratis og anonymt. Angriber de et system fra din forbindelse, så er det dit IP-nummer, der bliver registreret. I Frankrig, for eksempel, kan staten kræve af din udbyder, at du bliver afbrudt fra internettet og blacklistet, hvis dit IP-nummer viser sig at blive brugt til ulovlig download eller piratering. Man anser dig for ansvarlig, for hvad der udgår fra din forbindelse. Det er dit ansvar at sikre dig.

Denne form for piratering bliver brugt en del, fordi det er en dejlig måde at forblive anonym på. Selv om en del cafeer og offentlige steder tilbyder gratis wi-fi, bliver det sjældent brugt af pirater, da det er for offentligt.

Man betegner stadig væk denne metode som WarDriving (krigsførelse, imens man kører).

Oprindeligt var der også en metode kaldet WarChalking (krigsførelse, imens man går og markerer med kridt). Det var en metode, der blev opfundet af en gruppe venner i England i juni 2002.

Piraterne afmærkede med kridt i nærheden af de huse, hvorfra man kunne surfe gratis på nettet.

Faktisk har dette fænomen – indirekte – været årsag til et nyt koncept: Gratis internetcaféer, som dem vi har i Danmark og i mange andre lande i verden. En idé, vi faktisk kan takke piraterne for.

I dag bliver Warchalking benyttet cirka lige så ofte som man bruger musketter i moderne krigsførelse, men WarDriving eksisterer stadig væk. En pirat vil til hver en tid foretrække at hacke sig ind på en almindelig brugers netværk frem for at benytte sig af et for offentligt netværk, hvor han kan ses af mange.

netid	ssid	type	wep	trilat	trilong
00:12:17:D5:53:32	babaiaganatoiaga	infrastruc	Y	55.71001434	12.52168941
00:14:6A:17:C3:F0	KBH Skolernes HOTSPOT	infrastruc	N	55.71002197	12.53501797
00:14:7C:53:C8:AA	jufee	????	Y	55.71002197	12.53223228
00:04:75:64:77:01	3Com	infrastruc	N	55.71002579	12.52798843
00:14:6A:3D:3E:E0	KBH Skolernes HOTSPOT	????	N	55.71003342	12.53439713
00:02:72:51:82:EF	Jensen	infrastruc	Y	55.71003723	12.52789307
00:19:5B:47:98:C3	PP	????	Y	55.71003723	12.52810287
00:11:50:4F:EB:33	powernet	????	Y	55.71004105	12.52327156
00:13:10:83:75:B8	linksys123	????	Y	55.71004868	12.52877331
00:17:3F:07:31:02	Louise+Rasmus	????	Y	55.71004868	12.52849579

1-1. www.wigle.net – Et af disse netværk kan blive meget berømt, når det bliver offentliggjort på WarDriving internettet. Er det dit netværk? Det var da uheldigt!

Kendte eksempler

For bedre at forstå de forskellige facetter af hacking, og for at se forskellen mellem søndags-hackeren og eksperten, vil vi tage et eksempel. Eksemplet er over 10 år gammelt, men er et flot bevis på, hvor højt pirater kan ramme i systemet.

Vi kan tale om det så berømte angreb, som skete natten fra den 21. til den 22. oktober 2002 på *DNS-roden*.

Hvad i alverden er "DNS-roden"?

Alle domæner, som man bruger til at komme på en hjemmeside, **`www.google.dk`** for eksempel, administreres af en organisation, ICANN, gennem nogle "domæne-navne servere", de såkaldte *DNS*'er (Domain Name Server).

Alle kan have en DNS derhjemme: Det er et program, som er installeret på en computer, og som sammensætter et IP-nummer med et navn. For eksempel vil **`minhjemmeside.com`** svare til IP 192.168.0.2.

Dette er ændret lidt siden den 6. juni 2012, hvor vi officielt fik IPv6, men alt det taler vi lidt mere om senere. Ændringen er officiel, men endnu ikke gennemført allevegne, og der går nogle år før det er. Så lad os fortsætte med denne standard forklaring.

Der er mange sådanne lokalservere rundt om i verden, og de er ikke særlig interessante at angribe, da man ikke får ret meget ud af at kontrollere dem (om end idéen om at tvinge google.com eller microsoft.com til en anden server sandsynligvis har fristet mere end en).

Nej, det, som har interesseret hackerne, er de såkaldte root-servere. Disse maskiner har intet til fælles med firmaets eller hjemmets DNS-server. Der er tale om selve internettets struktur og arkitektur. At få dem til at ryste betyder at få hele nettet til at ryste.

Der findes 13 af disse servere. De hedder fra A.ROOT-SERVERS.NET til M.ROOT-SERVERS.NET og befinder sig rundt omkring i verden. Deres rolle er at forbinde alle de små domæne-servere på nettet med "efternavnet" på serveren.

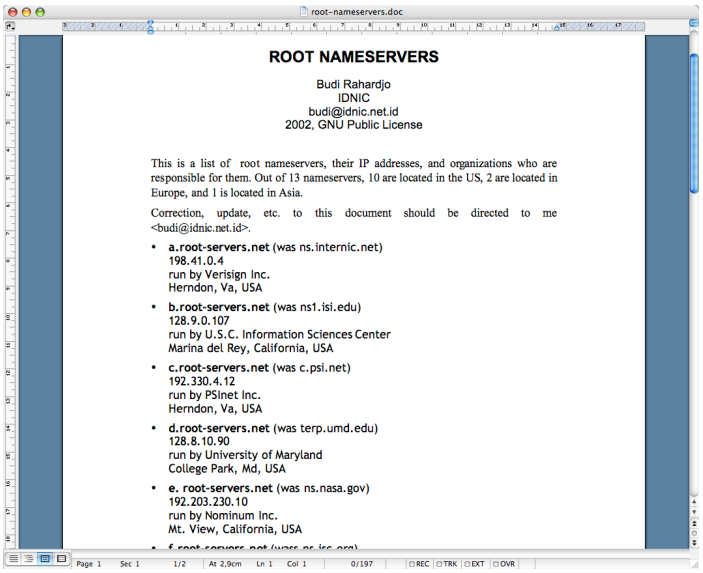
Dette betyder ikke, at der kun er 13 fysiske server (den 11. marts 2013 var der 359 fysiske servere). Men der er tale om 13 "logiske servere".

Hvis du fx ønsker at se **`www.usa.gov`**, så vil din efterspørgsel først sendes til den root-server, som styrer .gov'erne. Derefter vil denne server sende dig til den server, som registrerer gov-domænerne, som vil videresende dig til lokal-serveren.

Dette betyder, at hvis man blokerer .gov-serveren, så vil intet domæne med endelsen .gov være tilgængeligt. Groft sagt, hvis disse 13 servere gik i stå, vil stort set intet på internettet fungere (medmindre du er så heldig lige at huske IP-nummeret på den server, du vil besøge, naturligvis).

Disse meget vigtige servere er i overensstemmelse med internettets tankegang fuldt offentlige. De er ikke skjult, og det er yderst nemt at finde dem, få fat i deres IP-numre, deres referencer m.m.

Root DNS G og H fx, styres af det amerikanske militær. Jeg skulle ikke bruge mere end fem minutter for at identificere dem og finde en udførlig beskrivelse af deres system via en indisk server. Se selv på: **`budi.insan.co.id/articles/root-nameservers.doc`**


root-nameservers.doc

ROOT NAMESERVERS

Budi Rahardjo
IDNIC
budi@idnic.net.id
2002, GNU Public License

This is a list of root nameservers, their IP addresses, and organizations who are responsible for them. Out of 13 nameservers, 10 are located in the US, 2 are located in Europe, and 1 is located in Asia.

Correction, update, etc. to this document should be directed to me <budi@idnic.net.id>.

- **a.root-servers.net** (was ns.internic.net)
  198.41.0.4
  run by Verisign Inc.
  Herndon, Va, USA
- **b.root-servers.net** (was ns1.isi.edu)
  128.9.0.107
  run by U.S.C. Information Sciences Center
  Marina del Rey, California, USA
- **c.root-servers.net** (was c.psi.net)
  192.330.4.12
  run by PSInet Inc.
  Herndon, Va, USA
- **d.root-servers.net** (was terp.umd.edu)
  128.8.10.90
  run by University of Maryland
  College Park, Md, USA
- **e. root-servers.net** (was ns.nasa.gov)
  192.203.230.10
  run by Nominum Inc.
  Mt. View, California, USA

Page 1 Sec 1 1/2 At 2,9cm Ln 1 Col 1 0/197 REC TRK EXT OVR

1-2. Root-serverne er offentlige.

Det er på grund af denne "reklame" og et godt kendskab til servernes struktur, at pirater kunne angribe serverne den 21. og 22. oktober 2002. Hele roden, serverne A til M, blev med en vis succes angrebet af pirater, og syv ud af 13 servere holdt op med at fungere. Angrebet varede i cirka en time.

Selv om angrebet var omfattende, har det ikke rigtigt medført problemer på nettet. Der skal dertil siges, at der findes dubletter af disse servere rundt omkring på planeten, og der er tale om overordentlige kolosser, som ikke lige er til at få ned. *Verisign*s talsmand (Verisign er det firma, som administrerer en af disse 13 servere) har i øvrigt erklæret, at samtlige forespørgsler, der blev sendt til serverne, kunne være blevet klaret af blot én af disse servere.

Alle er ikke enige i det. Nogle mener, at hvis otte af disse servere har bugs, vil forespørgsler på domænenavne blive meget forsinket. Man ved stadig væk ikke i dag, hvem der angreb serverne.

For en god ordens skyld skal det nævnes, at serverne også blev angrebet den 6. februar 2007. Angrebet varede i 24 timer, og to root server (G-ROOT og L-ROOT) led meget under angrebet, og to andre servere (F-ROOT og M-ROOT) blev hårdt belastet.

Anonymous (en berygtet gruppe af script-kiddies) truede med at angribe serverne den 31. marts 2012, men det blev ved truslen, og intet er sket.

Som du selv vil se senere i bogen, kan man sagtens være anonym, imens man begår den slags, og hvis piraterne bliver ved med at holde tæt, er der yderst få chancer for, at vi nogensinde vil finde ud af, hvem der har gjort det.

Den angrebsmetode, der blev benyttet, var *DoS*, Denial of Service. DoS går ud på at bombardere serveren med *Ping* (forkortelse for Packet INternet Groper – Internet-pakke-tester).

Princippet bag Ping er, at man bruger det til at teste, om en server svarer, ved at sende den en pakke data. Ved at oversvømme serveren med forespørgsler sker der det, at på et tidspunkt kan maskinen ikke svare længere og går i baglås. Det er den slags angreb, som har taget Yahoo, eBay og Amazon offline for nogle år siden.

For at kunne lave den slags angreb skal man råde over overordentlig mange computere. Derfor har mange computere, der er smittet af trojanske heste, været

under piraternes kontrol og har deltaget i angrebet. Måske har din computer været med i et sådant angreb, uden at du ved det.

Det er her, man tænker på, at måske skulle man være noget mere påpasselig med sit system, ikke?

Den slags angreb kan få os til at spørge os selv: Hvem står bag?

Vi må lade det forblive ubesvaret. Angrebet kan sagtens have været udført af meget velorganiserede eksperter, lige så vel som det kan have været udført af en bande bøller.

Analyse af et typisk angreb

Jamen ... Hvordan gør de så?

Alle pirater benytter samme metode til at trænge ind i et system. Vi kan resumere et angreb i tre faser:

- ❑ Forberedelsen.
- ❑ Offensiven.
- ❑ Invasionen og besættelsen eller tyveriet.

Det lyder godt nok militæragtigt, og det er det også. Der er tale om en offensiv (angribende) handling udført af nogen eller nogle imod et system, der ikke tilhører dem.

Der findes flere grupper, som alle stiler mod hver deres mål: Vandalerne, som angriber blot for at ødelægge, guerillaer, som angriber for at vise, at de er de stærkeste, eller for at vise, at de eksisterer, og de regulære hære, som er organiseret af regeringer til at destabilisere fjendens hær, eller som bruges til spionage, som for eksempel Stuxnet eller Flame, som var direkte rettede imod de iranske atomkræftværker, fabrikker og infrastruktursystemer.

I 1991, under Golf-krigen, få minutter før at koalitionens styrker gik til angreb, var der absolut ingen data-anlæg og kommunikation, der fungerede i Irak. Landet var afskåret fra resten af verden.

I 2010 udspionerede ormen StuxNet de iranske atomkraftværker (og andre industrielle systemer), tog kontrol over dem, tog dem ned, altimens den simulerede, at alt fungerede fint. Det vil sige at for ham, der sad foran skærmen, så alt fjong ud, imens ormen i virkeligheden havde genprogrammeret dele af systemet.

I 2012 var det Flame, der blev afsløret. Ormen havde været i mellemøstens computere i flere år (det vides ikke hvor længe), fangede al kommunikation rundt omkring (ved hjælp af computerens webcam, mikrofon, m.m.), e-mail, browsing, og alt hvad man ellers bruger computeren til. Det viste sig, at også de mobiltelefoner (med bluetooth aktiveret), som var omkring, var ofre for Flame: Deres adressebog blev suget og eventuel kommunikation opsnappet.

Kort tid efter at Flame blev kendt af offentligheden, blev der sat en autodestruction sekvens i gang, så den forsvandt fra alles maskiner.

Måske mindre imponerende, men dog meget symbolsk, er det rygte (til dels bevist i øvrigt) om, at nogle kommunikationsfirmaer har den dårlige vane at installere *bagdøre* i nogle af deres systemer.

> **Bagdør: Indgangsdør i et system, som bevirker, at man kan omgå sikkerhedsforanstaltningerne. Nogle trojanske heste er bagdøre: De åbner din computer for den, der vil benytte sig af den, og giver vedkommende adgang til dit system eller dine harddiske.**

Vi går ud fra princippet om, at vi hverken er spioner, marketingseksperter, militærfolk eller politibetjente, men dette forhindrer os ikke i at konstatere, at vores netværk og computere er sårbare. Vi kan konstatere, at de, der angriber, kan gøre stort set, hvad de vil, og at det er yderst vigtigt at studere, hvordan disse pirater handler.

Forberedelse af et angreb

Før selve angrebet vil piraten skaffe sig oplysninger. Han skal vide, hvad og hvem han har med at gøre, så han kan udnytte hullerne.

Den første del af angrebet er derfor analysen: Ved at scanne, at sniffe, at spore *routen*, at bruge forskellige programmer, vil piraten forsøge at kortlægge netværket så præcist som muligt.

Naturligvis vil denne fase ikke give adgang til noget som helst. Men lige så vel som en biltyv bedst kender til den model, han plejer at stjæle, vil piraten foretrække at angribe et system, han kender i forvejen ... Han skal have sin Franz Jäger fra Berlin – så at sige.

Derfor skal din første handling være at begrænse de informationer, du giver fra dig, så meget som muligt. Af den grund skal du også bruge de samme værktøjer som han, så du kan identificere hullerne i dit system eller i dit netværk. På samme måde som han ville gøre det.

Piraten ønsker også at vide, hvordan systemerne kører, og hvem der ejer dem. Den nemmeste måde at få adgang til et netværk på er rent faktisk at have det officielle password og brugsanvisninger.

Denne fase kalder man for *social engineering*. Det er nærmest detektivarbejde. Tænk på, hvor mange oplysninger du giver fra dig, når du beder om hjælp til et bestemt problem. Fortæller du ikke om, hvilken computer du har, hvilken router og hvilket styresystem? Dette er kræs for den, der læser det.

Fup benyttes meget. Man kan nemt som pirat sende en e-mail og lade som om, man er en anden.

For eksempel kan man købe domænet mini-laan.com, som er tæt nok på det eksisterende: **`minilaan.com`**.

Man sætter en mailkonto op: **`hans.jensen@mini-laan.com`** og skriver derfra til administratoren om, at man har mistet sit password. Er administratoren blot lidt stresset eller uopmærksom, så kører det igennem. Man kan ligeledes med held bruge den slags metoder i store skoler eller store strukturer med flere administratorer.

Når piraten har fået de nødvendige oplysninger, er der kun tilbage at udføre angrebet.

Online

Jo flere oplysninger piraten er i besiddelse af, desto hurtigere og mere effektivt vil angrebet være.

Man kan dog angribe et system, selv om man kun har få informationer, og enten kontrollere det eller få det til at gå ned. Til det formål kan der bruges flere teknikker:

For at slå en computer ud vil man forsøge at udnytte systemfejl eller bruge et password, som man har fået fat i. Man kan også forsøge at udnytte TCP/IP-svagheder.

For at få adgang til en computer kan man enten udnytte et hul i systemet eller et password, som man har fået fat i eller har cracket sig vej til ved hjælp af et password-crackingprogram.

Vi vender tilbage til disse forskellige muligheder, som man kalder *exploits* (udnyttelser).

Hvis piraten er meget dygtig, vil han selv have skrevet pågældende program. Ellers, hvis det er en begynder-hacker, har han fået fat i det på sider på nettet eller via nyhedsgruppen `alt.2600`.

`http://astalavista.com` er en af de mest kendte ressourcer til information om sikkerhed for hackere.

`http://neworder.box.sk` er en ren mine fyldt med informationer og links, hvorfra man kan downloade programmer.

Jeg vil gerne slå fast, at hackerens yndlingsværktøj (og altså administratorens, så han kan beskytte sig!) er Google. Via den side kan du med lynets hast finde stort set en hvilken som helst information om pirateringens varmeste emner.

Naturligvis skal man kunne bruge Google, og det er ikke formålet med denne bog.

> **Stedet: Stedet, hvor undergrunden mødes, er en nyhedsgruppe, der hedder alt.2600. Der vil du finde pirater, it-verdenens journalister og højst sandsynligt også noget politi og spioner. Man kan finde alle mulige diskussioner om at bryde ind i forskellige systemer, telefonpiratering, hvordan man gennembryder forskellige anti-kopi-systemer samt nogle gode vitser (på engelsk). Du vil også kunne finde de nyeste værktøjer samt lyssky forretninger som køb af visakortnumre. De nyankomne henvises til FAQ (Frequently Asked Questions = Ofte Stillede Spørgsmål) her: www.faqs.org/faqs/alt-2600/faq/, og man sørger for at have læst den og forstået den, før man kaster sig ud i diskussionen.**
>
> **Hvis din udbyder ikke giver dig adgang til alt.2600, kan du få adgang til den via forskellige offentlige sider, som Google: http://groups.google.dk/group/alt.2600?hl=da**
>
> **Du kan også kaste et blik på: www.2600.com**

Leg og lær

For at kunne forstå pirateringens principper og for at kunne finde modtræk vil vi bruge de metoder, som bruges af pirater, og forsøge at trænge ind i vores eget system. Inden for it, ligesom inden for ethvert andet område, skal man kende angriberens metoder, så man bedst kan forsvare sig.

Dog er det vigtigt at minde læseren om, at piratering på en anden computer end din egen, eller piratering af en person, der ikke har givet dig tilladelse er ulovligt. Det kan komme til at koste dig dyrt at være uopmærksom på loven:

Når man er fyldt 15 år, kan man straffes, hvis man gør noget ulovligt. Hvis man er hacker, kan man få en bøde eller fængselsstraf på op til 6 måneder. I meget grove sager, hvor der er tale om hærværk af betydeligt omfang, kan man straffes med fængsel i op til 4 år.

De to mest brugte paragraffer i hackersager er straffelovens § 263 og § 291.

Den første paragraf handler om, at man kan straffes, hvis man læser andres personlige post, kigger i andres personlige gemmer eller hemmeligt lytter med på andres fortrolige samtaler.

Den anden paragraf handler om, at man bliver straffet, hvis man begår hærværk.

Man kan derudover risikere at skulle betale erstatning til den person eller virksomhed, det er gået ud over.

§ 263.

Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget

1) bryder eller unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet,

2) skaffer sig adgang til andres gemmer,

3) ved hjælp af et apparat hemmeligt aflytter eller optager udtalelser fremsat i enrum, telefonsamtaler eller anden samtale mellem andre eller forhandlinger i lukket møde, som han ikke selv deltager i, eller hvortil han uberettiget har skaffet sig adgang.

Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

Stk. 3. Begås de i stk. 1 eller 2 nævnte forhold med forsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særlig skærpende omstændigheder, kan straffen stige til fængsel indtil 4 år.

§ 291.

Den, som ødelægger, beskadiger eller bortskaffer ting, der tilhører en anden, straffes med bøde eller med fængsel indtil 1 år.

Stk. 2. Øves der hærværk af betydeligt omfang, eller er gerningsmanden tidligere fundet skyldig efter nærværende paragraf eller efter §§ 180, 181, 183, stk. 1 og 2, 184, stk. 1, 193 eller 194, kan straffen stige til fængsel i 4 år.

Stk. 3. Forvoldes skaden under de i stk. 2 nævnte omstændigheder af grov uagtsomhed, er straffen bøde eller fængsel indtil 6 måneder.

Husk, at legen kan blive til alvor, hvis du misbruger viden.

Tjek lige: **`www.kriminalitet.dk/loven.html`**

Sagt på en anden måde: Alle de ting, du kan finde på at gøre på en anden persons computer med de værktøjer, du får her, kan medføre straf.

Jeg kan allerede høre de første Karl Smarter, der griner. Pas på! Din arbejdsgivers computer, dine venners computer, dine fjenders computer, regeringens, bankens computere osv. har alle logs, som kan læses og fortælle klart og tydeligt, hvem gjorde hvad.

Politiet ved udmærket, hvem de skal spørge for at spore et IP-nummers ejer.

Da jeg skrev denne bog, befandt programmerne sig på min computer eller vores netværk eller server. Hvis der blev brugt systemer udefra, har det altid været med modpartens viden og accept.

Leg og lær ... på dine egne maskiner, ikke på andres. Eller tag de eventuelle, ubehagelige, konsekvenser, der uvægerligt vil følge med.

Når det nu er sagt ... Lad os gå i gang!