Chill

Wi-fi-hacking

Hemmelighederne bag Wi-Fi-hacking

Wi-Fi betyder Wireless Fidelity

Nej!

Det er en vandrehistorie. Selv om Wi-Fi ligner Hi-Fi, så betyder Wi-Fi ikke Wireless Fidelity. Det siger i hvert fald Phil Belanger, som er fra Wi-Fi Alliance.

Han er fra Interbrand Corporation, som er det firma, der udviklede mærket og logoet Wi-Fi, som bliver brugt til at beskrive WLAN produkter, som bygger på IEEE 802.11 standarden.

Ifølge Belanger blev mærket Wi-Fi og det Yin-Yang-agtige logo opfundet af Interbrand.

Dengang havde Wireless Ethernet Compatibility Alliance (som nu hedder Wi-Fi Alliance) hyret Interbrand for at finde navn og logo, fordi de ville have et navn lidt mere spændende end ”IEEE 802.11b Direct Sequence”.

Wi-Fi Alliance har brugt Wireless Fidelity i et slogan: ”The Standard for Wireless Fidelity”, men de fjernede det fra deres marketing og går imod, at man spreder idéen om, at Wi-Fi skulle betyde det.

Der findes ingen standardskrivemåde for Wi-Fi. Og man kan skrive næsten stort set, som man vil: WiFi, Wi-Fi, wifi ...

Da der er tale om et mærke, og da Wi-Fi Alliance selv bruger skrivemåden ”Wi-Fi”, har jeg holdt mig til det.

1. Introduktion til Wi-Fi-hacking

> **Wireless local-area networks, som ofte kaldes for WLAN, Wi-Fi-netværk eller trådløse netværk, er blevet standard i ethvert hjem. Stort set enhver bruger har sit trådløse netværk. Man finder det alle vegne, fra butikker til hoteller, til netværkscaféer ... Trådløse netværk er blevet så almindelige, at man forventer dem allevegne.**

Det er sandt, at Wi-Fi er en meget god ting. Dels er det mere praktisk, fordi man er fri for en masse ledninger, det er ofte billigere at implementere end trådet netværk (især for store firmaer), og så er det meget fleksibelt.

Så jo, vi skal regne med, at den trådløse teknologi er den nye standard og vil blive med os i mange år endnu.

Men hvor sikker er denne teknologi egentlig?

> **IEEE 802.11**
>
> **Man hører ofte om IEEE 802.11, når der tales om trådløse netværk.**
>
> **IEEE 802.11 står blot for Institute of Electrical and Electronics Engineers (IEEE). Standarden fik nummer efter gruppens navn og det år og måned, gruppen blev udformet i: februar 1980. Tallet .11 svarer til undergruppens nummer.**

Man kan afgjort se, at firmaer, der sælger trådløse netværk, har vind i sejlene, og at man kan finde trådløse i stort set enhver firma eller hjem.

Den succes standarden har fået er faktisk større, end IEEE havde regnet med, og som vi ser jævnligt med Microsoft, jo større man er, des flere angreb skal man regne med at få.

Sammen med de besparelser og den øgede produktivitet, som man får med trådløst netværk, kommer der en del sikkerhedshuller.

Der er ikke tale om de almindelige sikkerhedshullersom vi ellers kender dem, såsom SpyWare, svage password og manglende patch[1], om end disse problemer også findes dér. Nej, trådløse netværk åbner for en helt ny verden af muligheder for en pirat.

Dette bringer os til formålet med denne bog: Her taler vi om White Hat-hacking (som af og til bliver kaldt Gray Hat-hacking).

Det vil sige, at du vil lære at bruge hackerværktøj og finde de svage punkter i et system.

Formålet med det er, at du enten kan fortælle den person, der ejer netværket om systemets svagheder, eller også er det dit eget system, og dér kan du gøre, hvad du vil.

Husk at have en aftale med den ejeren af det netværk, du tester, helst skriftligt. Du skulle nødigt få problemer.

[1] Se bogen Hackerguiden 2.013 for flere oplysninger om den slags huller.

White Hat, Gray Hat og Black Hat

En White Hat er en "god hacker" vil man sige. Det vil sige en, som synes, det er sjovt at hacke ting, fordi det er en udfordring. White Hat vil ikke offentliggøre oplysninger om et fundet sikkerhedshul før efter, at den person eller system, der er ramt af det, har fået en mulighed for at lukke hullet. Af og til vil en White Hat oven i købet være en behjælpelig med det.

White Hat kaldes af og til Gray Hat, da nogle mener, at White Hat er Gray Hat, der arbejder for en regering eller et firma.

Black Hat er pirater, som er ude på at smadre andres computere, hjemmesider, stjæle oplysninger eller andet.

I denne bog vil du lære at forstå de forskellige trusler og huller forbundet med 802.11, og hvordan du kan hacke dem og sikre dem.

I dette første kapitel skal vi se lidt på de mest almindelige trusler, og jeg vil vise dig nogle vigtige sikkerhedsværktøjer, du skal bruge og teste dit system med.

Jeg krypterer – hvorfor skal jeg teste?

Siden sidst i 90'erne har det trådløse system været kendt for at være usikkert. Der er en lang historie af svagheder, krypteringssvagheder, authentification-problemer m.m. Problemet er så svært at have med at gøre, at der er blevet lavet to ekstra standarder for at tilbagevise angreb. Disse er:

- **Wi-Fi Protected Access (WPA):** Denne standard blev udviklet for at rette på den såkaldte og velkendte WEP-svaghed (mere om den senere), indtil IEE kom med 802.11i standarden.
- **IEEE 802.11i (omtales som regel som WPA2):** Dette er den officielle standard, som indbefatter patch for WEP sammen med andre krypteringsmekanismer, som skal sikre trådløse netværk.

Disse standarder har løst en del af de sikkerhedsproblemer, man har med protokollerne 802.11a/b/g.

Problemet er ikke, at disse løsninger ikke virker, men at alt for mange netværksadministratorer er konservative og har stærk modstand mod forandringer og derfor ikke implementerer disse ændringer i deres systemer.

Du skal tænke på, at en systemadministrator skal opdatere samtlige de eksisterende systemer, og mange ønsker ikke at gå i gang, da de er bange for, at deres system bliver endnu sværere at styre.

Mennesket er som oftest det svageste led i et netværk, og menneskers frygt for forandringer og hårdt arbejde gør, at mange systemer rundt omkring er lige til at kompromittere.

Husk også, at i nogle firmaer vil man finde en eller andet Karl Smart, som vil tage sit eget udstyr med, eventuelt endda en router eller Access Point, for at forbigå nogle af administratorens begrænsninger.

Da deres eget system langt fra er sikkert, kan disse personer ligeledes kompromittere hele netværket.

Derfor, hvis du er administrator på et større netværk, skal du faktisk være paranoid og streng: Tjek jævnligt for den slags, og slå ned med hård hånd på den slags adfærd. Det vil til hver en tid være bedre for dig at have ry for at være en idiot frem for at risikere hele netværket.

Hvad kan der så ske?

”Nå ja ... Lidt hysterisk”, tænker du måske. ”Jeg har ikke noget vigtigt på min computer alligevel”, eller ”Hvorfor i alverden skulle nogen være interesseret i min computer, der er ikke mange chancer for det”.

Tjoh ... Der kan ske en del ting (og siden du læser denne bog, så tænker du nok ikke sådan alligevel). Det, du udsætter din computer og netværk for, inkluderer følgende:

- ❏ Fuld adgang til de filer, som er på serveren, eller som bliver overført til eller fra serveren.
- ❏ Tyveri af passwords.
- ❏ Opsnapning af e-mails.
- ❏ Bagdøradgang til dit trådede netværk.
- ❏ DoS (Denial of Service) angreb, som vil få dit system ned og forsinke dit arbejde.
- ❏ Ulovligheder begået fra din computer eller fra dit netværk.
- ❏ Zombier: Din computer bliver brugt til at angribe en anden, så du ser ud til at være den slemme fyr.
- ❏ Spamming: En spammer kan bruge din e-mail-server til at sende spam, spyware, virusser eller andet.

Der er en del andre muligheder, naturligvis. Det, der kan ske med dit trådløse netværk, og det, det kan bruges til, er nogenlunde det samme som det, et trådet netværk udsættes for. Der er bare den forskel, at man er mere udsat med et trådløst, da en pirat kan være i en bil i nærheden og lave ballade. Vedkommende behøver ikke længere at have fysisk adgang til en computer.

Det største problem er dog at uden det rette (og dyre!) udstyr og uden nærmest paranoid næsten konstant netværkstjek, er det stort set umuligt at finde en uvedkommende i ens system. Du kan ikke vide, om vedkommende er for enden af gaden, i bygningen ved siden af eller et par kilometer væk.

Det kan være en nysgerrig nabo, som bruger frekvensen for at høre dine trådløse telefoniske samtaler, eller en kollega, som blander sig i noget, der ikke vedrører ham.

Vi er så vant til trådet netværk, at vi sjældent tænker over alt det, der kan aflyttes for den, der har ører ...

Forstå din fjende

For at bedre kunne beskytte dit system skal du rent faktisk tænke som en pirat, selv om det kan forekomme svært, fordi mange af os (de fleste, heldigvis!), ikke vil kunne finde på at skade andre.

Men fordi du ikke er sådan, betyder det ikke, at nogle andre ikke kan finde på det. Derfor bliver du nødt til at sætte dig lidt ind i den skadelige tankegang for bedre at kunne forsvare dig. Sådan er det såmænd med alt. Det er, fordi du tænker over det, der kan ske med dit hjem, at du låser, når du går.

I første omgang gælder det om at være klar over, at der er mange – rigtig mange – ubeskyttede systemer rundt omkring. Og husk, at langt de fleste Black Hat egentligt ikke er så fantastisk dygtige. De fleste af dem er script-kiddies, som bare er ude på at more sig.

Script-kiddies er til internettet det, hærværkere er til en lørdag aften: De synes, det er sjovt at smadre ting. Derfor har de som oftest ikke disciplin nok til at lære nyt (eller til at lære i det hele taget) og de går gerne efter færdiglavede scripts, som de bare bruger uden at være helt klar over, hvordan tingene fungerer (deraf navnet script-kiddies, "script-knøse").

Den store fordel ved dem er, at hvis de blot møder lidt modstand, så vil de lade dit system være i fred. Det typiske offer vil være det lille firma med kun en eller to Access Points eller et enkeltmandsfirma eller en privat person.

Det er det af flere årsager:

- Små firmaer eller privatpersoner vil sandsynligvis ikke have en systemadministrator.
- Små netværk vil højst sandsynligt beholde standardindstillinger.
- Små netværk vil højst sandsynligt ikke have jævnlige netværkstjek og ikke have et system til at feje netværket for at finde uvedkommende. De vil sandsynligvis ej heller have WPA eller WPA2, for de vil mene, at det er overdrevet (eller ganske enkelt fordi de slet ikke ved, hvordan man sætter det op).

På den anden side skal store netværk heller ikke føle sig sikre. Det er blot andre ting, der gør det nemt at piratere store netværk:

- Det er nemmere at cracke den såkaldte Wired Equivalent Privacy (WEP) nøgle på store netværk. Det, fordi man som regel finder krypteringnøglen ved at analysere de netværkspakker, der cirkulerer på netværket, og jo større er netværk, des flere pakker er der, og des hurtigere og nemmere er det at cracke WEP-nøglen. Der er et kapitel om WEP-cracking senere i bogen, så fortvivl ikke!
- De fleste netværksadministratorer har hverken tid eller lyst til at tjekke netværket for at se, om der befinder sig uvedkommende på det.
- Det er meget nemmere at gemme sig i en bil på en stor parkeringsplads med sin computer end på en lille gade uden for dine vinduer. For lad os være logisk: Ville du ikke være mistænksom, hvis du så en bil med en stor antenne på taget og en fyr med en bærbar parkeret lige uden for dine vinduer? Sæt samme mand med samme bil på en parkeringsplads med 2.000 pladser uden for et stort supermarked, og det bliver lige straks mindre mistænkeligt (og i hvert fald vil lange de fleste forbipasserende være ligeglade).

- De fleste store organisationer bruger de antenner, der følger med deres Access Point (det gør vi andre også, men vi køber ikke så kraftigt materiale), og de tænker ikke så meget over, hvor meget der stråler uden for bygningen.
- I langt de fleste store firmaer er det trådløse netværk en forlængelse af det trådede netværk. Det vil sige, at når man får adgang, får man også adgang til det trådede netværk, og der er mindst lige så mange spændende ting at finde der, som i det trådløse. Måske mere.
- Langt de fleste store systemer er sat op efter nogle standardrutiner, som ofte er de samme. Det er som regel: stoppe Service Set Identifier (SSID), der som regel udsender netværkets navn rundt omkring og aktiverer Media-Access Control (MAC) filtrering, hvilket filtrerer de computere, der må forbinde sig ved hjælp af det nummer, der er brændt inde i deres netværkskort. Langt de fleste ved ikke, at de to ting er uhyre nemme at forbigå. Det ser vi også på.
- SSID er som oftest navngivet enten efter firmaets navn eller efter den afdeling (endnu bedre), for så ved piraten faktisk, hvilket system han skal angribe først.

Naturligvis er det ikke fordi disse ting kan forbigås, at de ikke skal bruges. Vi ved alle, at der eksisterer ingen absolut sikkerhed på noget som helst netværk, men det betyder ikke, at man ikke skal gøre noget ved det. Selv om alle biler kan stjæles, låser du alligevel din bil, før du går fra den.

Du vil nok aldrig kunne undgå alle former for angreb, og du kan ikke forsvare dig mod et angreb, der ikke er sket endnu, men du kan forberede dig, vanskeliggøre det, så kun ganske seje pirater kan komme igennem, og så kan du lære at formindske tabet, hvis angrebet sker.

Det er lidt som en kold krig. For dem fra min generation, der kan huske, at der var en mur mellem Øst- og Vestberlin, og at der på et tidspunkt var en farlig optrapning af kernevåben, så kunne verden omkring trådløs hacking minde lidt om det.

Piraten finder et angreb, vi finder en parade, de finder et nyt angreb, osv. Man skal aldrig sove på sit grønne øre og mene, at nu hvor vi har sat en parade op, kan der ikke ske noget.

Lige før vi skal i gang

Nu er det på tide at se lidt på, hvordan vi skal gribe sagen an.

God hacking er nødvendigvis planlagt. Planlægning er:

Først få tilladelsen af din boss, den ansvarlige eller den, der ejer systemet, før du roder med det her. Husk det, da du kan falde over en ”honeypot” (altså en fælde for at tiltrække pirater), og du vil få svært ved at lade andre tro på dine gode hensigter, hvis ikke du har et eller andet skriftligt om det.

Find ud af, hvad der er dit mål.

Finde ud af, hvilke test og programmer du skal bruge og køre.

Værktøjet

Du skal også have dit udstyr parat, dit værktøj, for at kunne arbejde. Du skal som regel bruge mere end et program for at nå dit mål. Lad endelig være med at tænke som en Windows-dosmer og tro, at du kan have alt værktøj i et eller to programmer.

Du vil se rimelig jævnligt, at du kan få falsk positive resultater, som falsk negative resultater på en test. Det vil sige, at et program vil fortælle dig, at der er et hul dér, hvor der ikke er noget, eller omvendt.

Her er de vigtigste værktøjer, som bruges af den typiske pirat:

- ❑ Google (Jeps! Her begynder vi ofte!)
- ❑ En bærbar computer.
- ❑ Et GPS-system.
- ❑ Network Stumbler – Program til at finde netværk.
- ❑ AiroPeek – program til at analysere netværk.
- ❑ QualysGuard – program til analyse af sikkerhedshuler.
- ❑ WEP crack – program til at cracke kryptering

Vi vil se i detaljer på alle disse programmer, naturligvis. Det er vigtigt, at du ved, hvordan du bruger de enkelte værktøjer. Dels for at kunne sikre dit system, dels fordi nogle af disse værktøjer faktisk kan lave ravage i et system, og det er vi ikke interesseret i.

Alt i alt er der tre former for angreb, vi kan udføre mod et system.

De ikke-tekniske angreb

Det er de angreb, hvor man udnytter den menneskelige svaghed. Ting som dovenskab, ligegyldighed, ansvarsløshed og så naivitet, naturligvis.

Disse angreb kan indbefatte:

- ❑ At bryde ind i en computer, som en eller anden i firmaet har taget med sig for derved at få adgang til netværket.
- ❑ Social Engineering, når man lader som om, man er en anden person for derved at få oplysninger om et givent system.
- ❑ Fysisk set få adgang til antennen eller andet hardware og omkonfigurere det eller opsnappe data fra det.

Netværksangreb

Der er forskellige teknikker, der kan benyttes for at bryde ind i dit netværk eller, hvis ikke det kan lade sig gøre, for at smadre det. Netværksangreb er bl.a.:

- ❑ Installere en Access Point og fuppe de trådløse computere til at forbindes til den.
- ❑ Fange data fra netværket på afstand ved at gå omkring det, køre ved siden af eller flyve over det.
- ❑ Angreb på netværket ved at fuppe en lovlig MAC-adresse, bruge metoden ”Man In The Middle” (dvs. indsætte en computer mellem Access Point og computeren) m.m.
- ❑ Udnytte netværksprotokoller som SNMP.
- ❑ Lave et DoS-angreb (Denial of Service).
- ❑ Lave en jamming af signalerne.

Softwareangreb

Som om alt det ikke var nok, så er der på de forskellige maskiner også en del programmer, som er åbne for angreb. Disse kan være:

- ❑ Hacke sig ind på en maskines styresystem og andre programmer på en trådløs computer.
- ❑ Bryde ind via standardindstillingerne såsom passwords og SSID, som er sat til af producenten og ikke ændret.
- ❑ Cracke WEP-nøgler.
- ❑ Få adgang ved at udnytte et svagt authentificationsystem.

Vi vil se de fleste af disse metoder.