Honey

Frank Brokken
f.b.brokken@rc.rug.nl

ICT-security

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

Eerder, in Pictogram 2 (april/mei) van dit jaar heb ik 't al eens kort over honeypots en honeynets gehad: een door Lance Spitzner aan het arsenaal technieken dat security teams ter beschikking staat toegevoegde techniek die verdacht veel lijkt op een bekende manier om vliegen te vangen. Maak het voor de onverlaten zo aantrekkelijk dat ze massaal op je val afkomen, waarin hun veile acties in de gaten worden gehouden, zodat we bij productiesystemen weten waar we op moeten letten.

Ergens in je netwerk plaats je een aantal computers, die geen andere operationele functie hebben dan er te zijn. Er worden geen security patches op geïnstalleerd, er worden geen speciale beveiligingsmaatregelen op toegepast. Maar ze worden wel nauwkeurig in de gaten gehouden. Omdat deze systemen geen internetverkeer horen te genereren, is elk verkeer in principe verdacht en het begin of gevolg van een inbraak.

Cursus Honeynets

Hoe zoet die honing is, bleek onlangs nog. In de week van 6 oktober werd in de Zernikeborg de landelijke cursus 'Honeynets' georganiseerd. Eigenlijk moet ik zeggen: de 'internationale cursus Honeynets', want één van de deelnemers was afkomstig uit België, en de docenten waren afkomstig uit Brazilië.
Ik ontmoette Klaus Steding-Jessen en Cristine Hoepers tijdens het 15e FIRST congres, afgelopen juni in Ottawa. Beiden zijn bezig met de afronding van hun proefschrift over Honeynets, en ze presenteerden tijdens het FIRST congres een uitermate boeiend paper over hun ervaringen.
De idee om Klaus en Cristine uit te nodigen om in Groningen een cursus Honeypots/Honeynets te verzorgen ontstond korte tijd later, en zowel de directie RC als SURFNet reageerden enthousiast. Gelukkig niet alleen zij, maar ook Klaus en Cristine waren bereid om naar Groningen te komen.

Uiteindelijk moesten we een aantal potentiële deelnemers teleurstellen vanwege capaciteitsproblemen: we moesten de inschrijving stoppen nadat zich ruim 30 deelnemers hadden aangemeld.

Honeypot

Zodra een honeypot is geïnstalleerd (dus nog geen honeynet; zie ook **www.citi.umich.edu/u/provos/honeyd/**), dan kan het detecteren van ongewenste activiteiten beginnen. Tijdens de eerste dagen van de cursus lag de nadruk op het gebruik van honeypots: het `honeyd'-programma simuleert willekeurig besturingssystemen en server-faciliteiten, zonder dat die besturingssystemen en -faciliteiten feitelijk bestaan.
Het is opmerkelijk wat er dan zoal voorbij komt. In een paar dagen tijd ontving 'mijn' honeypot 111 BLASTER-wormen, 9 KUANG-wormen, en werden in totaal ruim 180.000 (!) verbindingen met de honeypot gemaakt vanaf computers die niet bij de cursus zelf

Frank Brokken (rechts) met de Braziliaanse docenten

De volle cursus

De lege practicumzaal

betrokken waren. Dat is opmerkelijk, omdat het bestaan van de honeypot nergens op het internet is vermeld: alle verkeer naar de honeypot is daarmee in principe verdacht.
En dat verkeer blijkt terecht verdacht te zijn, wanneer je kijkt naar het grote aantal wormen en virussen dat we in een paar dagen tijd voorbij hebben zien komen. Merk op dat mijn getallen op slechts één computer betrekking hebben. De computers die door de andere deelnemers zijn gebruikt hebben uiteraard vergelijkbaar intensief internetverkeer waargenomen.
Ten dele zal die informatie overlap vertonen met de aanvallen die op mijn honeypot zijn uitgevoerd, maar elke honeypot zal ongetwijfeld ook een aantal unieke inbraakpogingen te verwerken hebben gekregen.

Honeynet

De tweede helft van de cursus was zo mogelijk nog interessanter: een honeynet wordt gevormd door een groepje computers die op een standaard manier worden ingericht, en vervolgens met de nodige externe beveiligingsmaatregelen aan het internet worden gekoppeld. Die beveiligingen bestaan uit een zogenaamde gefilterde brug, die zich gedraagt zoals een frase uit een nummer van de popgroep de Eagles: `You can check out any time you want, but you can never leave'.
De gedachte is hier dat hackers in staat worden gesteld om hun kennis bot te vieren op standaard geïnstalleerde computers, maar van daaruit geen schade elders kunnen aanrichten. Boeiend (`pun intended')! Op die manier krijgen we inzicht in het doen en laten van de hacker: hoe komt men binnen? Wat doet men? Waar komt men vandaan? Waar wil men naartoe?
In een aangrenzend practicumlokaal werd het honeynet geconfigureerd. Bij herhaling heb ik de schijnbaar lege en ongebruikte zaal moeten verdedigen tegen collega's die veronderstelden dat de practicumzaal niet in gebruik was. In feite waren de computers in die zaal druk bezig om het doen en laten van hackers in de gaten te houden. En die zijn er, reken maar!

Op de honeynet-foto is de lege practicumzaal goed te zien. De meest rechtse computer op de tweede rij is een Windows 2000-server die onder andere door ondergetekende is ingericht. Op de overige computers waren weer andere besturingssystemen ingericht. Alle systemen waren `out of the box' geïnstalleerd: de leverancier biedt een installatie-cd aan en met die cd wordt het systeem geïnstalleerd. Vaak is dat de manier waarop een systeem aan het internet wordt gekoppeld. Helaas is dat niet altijd de meest verstandige manier, zoals blijkt.

Gehacked

Na afloop van de cursus waren alle systemen gehacked. Dat betekent dat we ervan uit moeten gaan dat een computer die van een cd wordt geïnstalleerd onveilig is, en binnen afzienbare tijd wordt gecompromitteerd. Hoe snel dat gebeurt, hangt een beetje af van het gebruikte besturingssysteem. De meest populaire systemen zijn ook bij de hackers het meest populair.
Onze Windows-2000 server was binnen een half uur bevolkt door diverse hackers. Niet één hacker, maar een aantal. Dit gegeven werpt natuurlijk vragen op: hoeveel universitaire computers zijn er op dit moment feitelijk overgenomen door hackers?
We weten uit de Honeypot/Honeynet-ervaring dat een deel van de inbraakpogingen afkomstig was vanaf universitaire systemen. Mijn collega Kees Visser onderhoudt een eigen Honeypot, en stuurt mij regelmatig informatie over RUG-systemen die zijn Honeypot met ongewenst bezoek hebben vereerd.
Een andere vraag: security patches worden meestal via het internet gedownload. Maar daarvoor heb je een internetverbinding nodig. Zodra de internetverbinding er is, ontstaat er een `race conditie': wie is het eerst binnen, de hacker of de security patch?

Moraal: het internet is nog onveiliger dan we altijd al dachten, en waarschijnlijk zijn meerdere RUG- en thuis-computers overgenomen door hackers. Honeypots vergroten het inzicht in de activiteiten van de hackers. Onlangs werd een oud student `betrapt' bij het bezoek van een Honeypot. Hij merkte dat-ie op een honeypot terecht was gekomen, maar toen was voor hem het kwaad al geschied. In dit geval was er niks ernstigs aan de hand, maar het voorval laat zien hoe behulpzaam een honeypot kan zijn bij het detecteren van de activiteiten van hackers.

Tenslotte, aan het einde van onze cursusweek kregen de deelnemers nog een cd, gevuld met zo'n 550 Mb nuttige informatie over Honeypots, mee naar huis. Met dank aan het RC Servicecentrum, die in een paar uur op de vrijdagochtend 40 cd's beschikbaar heeft weten te maken. 40 cd's met ruim 30 deelnemers: er zijn nog een paar cd's over. Ze zijn beschikbaar voor geïnteresseerden. Neem desgewenst contact op.