Stealth

ICT-security

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

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.

De F-117A Nighthawk 'Stealth' is, volgens het door de US Air Force gepubliceerde *fact sheet* (**www.af.mil/news/factsheets/ F_117A_Nighthawk.html**) het eerste vliegtuig ter wereld dat gebruik maakt van 'low observable stealth technology'.

Het bijzondere van de stealth-technologie is dat die technologie het mogelijk maakt om vrijwel onzichtbaar voor (vijandelijke) radarapparatuur binnen te dringen in vijandelijk gebied. Volgens de fact sheet:
"*The F-117A Nighthawk is the world's first operational aircraft designed to exploit low-observable stealth technology. This precision-strike aircraft penetrates high-threat airspace and uses laser-guided weapons against critical targets.... The F-117A program demonstrates that stealth aircraft can be designed for reliability and maintainability. It created a revolution in military warfare by incorporating low-observable technology into operational aircraft.*"

De achterliggende gedachte hier zal duidelijk zijn: als je niet kunt worden waargenomen, is het eenvoudiger om offensieve (of defensieve) taken succesvol uit te voeren dan wanneer je wel door 'de vijand' wordt gezien.
Het aardige is dat deze aanpak oppervlakkig gezien in strijd lijkt te zijn met een centraal principe uit de wereld van de beveiliging: Zwicky et al. (2000, zie afbeelding) schrijven (p.71): "*Security through obscurity is the principle of protecting things by hiding them*".

Er zijn allerlei redenen waarom 'security through obscurity' van twijfelachtige waarde is. Bijvoorbeeld: het geeft je een vals gevoel van veiligheid, of: het is de enige beveiliging die wordt gehanteerd. In combinatie met andere vormen van beveiliging kan 'security through obscurity' echter erg effectief zijn, zoals blijkt bij de F-117.

Rond het verschijnen van deze Pictogram vindt in Ottawa de 'Annual Computer Security Incident Handling Conference' plaats (**www.first.org/conference/2003/**). Op het programma staat onder andere de presentatie (door ondergetekende) van het programma STEALTH: opnieuw stealth-technologie, maar dan toegepast op computers.
Uiteraard hebben we het hier niet over het werpen van bommen, en het minimaliseren van radarprofielen, maar over een hulpmiddel ter beveiliging van computers.

'Onze' STEALTH is een zogenaamde 'File Integrity Checker', en is gebaseerd op een idee van Hans Gankema en Kees Visser, medewerkers van het RC.

Als een van de laatste verdedigingslinies die we kunnen opwerpen tegen inbrekers in onze computersystemen (hackers) kunnen File Integrity Checkers worden toegepast.

Het werkingsprincipe van de File Integrity Checker is eenvoudig en gebaseerd op het gegeven dat hackers vrijwel altijd software wijzigen, toevoegen of verwijderen op het systeem waarop ze hebben ingebroken, om zo een vrije toegang voor zichzelf te garanderen of om hun eigen aanwezigheid op het systeem te verbergen. Alle soorten systemen (Windows, Unix, Linux, Apple, etc.) kunnen hiermee te maken krijgen.

De File Integrity Checker dient in eerste instantie te worden toegepast op een 'schoon' systeem, waarop nog niet is ingebroken. De Checker bepaalt dan kenmerken van de software die op de gecontroleerde computer is geïnstalleerd. Zodra de hacker de software wijzigt, veranderen de kenmerken van de geïnstalleerde software, en bij een volgende 'run' van de Checker worden de wijzigingen gedetecteerd, en kunnen alsnog tegenmaatregelen worden genomen.

Een elegant concept, maar problematisch doordat de hacker de Checker zelf, of het bestand waarin de kenmerken van de software zijn opgeslagen ook kan wijzigen. Opslag van de gegevens op een 'read-only medium', zoals een cd-rom lost dat probleem weliswaar op, maar is toch ook lastig omdat na een onderhoudsbeurt van de software (bijvoorbeeld bij het installeren van een nieuwe versie) een nieuwe cd-rom moet worden gebrand.

Bij STEALTH wordt een andere aanpak gevolgd: vanuit een aparte computer (de *monitor*) wordt een beveiligde verbinding tot stand gebracht met een computer waarvan we de integriteit willen controleren (een *client*). De monitor geeft vervolgens aan de client de opdracht om z'n eigen software te controleren.

Het aardige is nu, dat het resultaat van deze controle beschikbaar komt op de monitor. De hacker die inbreekt op de client vindt dus nergens het bestand waarin de kenmerken van de software zijn opgeslagen, en vindt ook geen software die erop wijst dat de client wordt gecontroleerd. Een briljant concept.

We hebben STEALTH in vrij korte tijd kunnen ontwikkelen en gebruiken STEALTH inmiddels om een aantal computers, voornamelijk computers die server-taken vervullen, te controleren.

De naam STEALTH was snel gevonden: de monitor is immers vrijwel onzichtbaar voor hackers die inbreken op clients. Onze STEALTH is echter geen F-117 bommenwerper. Het heeft dan ook wat moeite gekost om een passende betekenis voor STEALTH te vinden. Uiteindelijk hebben we het volgende gevonden: 'SSH-based Trust Enforcement Acquired through a Locally Trusted Host'.

'SSH-based' heeft betrekking op de aard van de beveiligde verbinding tussen de client en de monitor. 'Trust Enforcement' op het toegenomen vertrouwen dat we hebben in de integriteit van de software die op de client is geïnstalleerd. De 'Locally Trusted Host' is de monitor: lokaal wordt de monitor vertrouwd: vanuit de monitor kan alle software op de client worden
bereikt en onderzocht.

Wie meer wil weten over STEALTH: de software is onder de open-source licentie ontwikkeld. STEALTH en de bijbehorende documentatie kan worden gedownload van **ftp.rug.nl/contrib/frank/software/linux/stealth**.

Het is uiteraard ook mogelijk om met vragen over STEALTH rechtstreeks contact op te nemen met: Frank B. Brokken, Security Manager (niet onzichtbaar).

Literatuur:

Zwicky, E.D., Cooper, S., Chapman, D. B. (2000), *Building Internet Firewalls*, O'Reilly, Sebastopol, ISBN 1-56992-871-7.