HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Diplomarbeit

Abteilung	**Informatik**
Name der Diplomandin / des Diplomanden	**Christian Bernet** **René Herrmann**
Diplomjahr	**2003**
Titel der Diplomarbeit	**Inside Out Attacke / DNS Tunnel**
Examinatorin / Examinator	**Ivan Bütler**

Kurzfassung der Diplomarbeit

Gemäss verschiedensten Studien werden 80% der Computer Attacken von internen Netzwerken der Unternehmen gestartet. Zum einen geht man davon aus, dass diese Attacken von frustrierten und in IT Belangen kompetenten Angreifer ausgehen - zum anderen werden auch Personen und Computer durch Viren und Trojaner unbewusst zu potenziellen Hackern.

Diese Diplomarbeit lässt die Frage offen, **wie** ein potenzielles bösartiges Programm im internen Netzwerk einer Unternehmung ausgeführt wird. Es interessiert die Frage, **was** das bösartige Programm anstellen könnte. Die Zielsetzung eines Trojaners lässt sich in folgende drei Kategorien gliedern:

Beschaffung, Veränderung und Zerstörung von Daten

- Beschaffung, Veränderung, Zerstörung von Daten
- Versand von Daten ins Internet
- Initiierung einer Remote-Control Verbindung, damit ein Hacker im Internet das korrumpierte System interaktiv kontrollieren kann

Im Fachjargon werden obige Attacken als "**Inside-Out**" bezeichnet, da der Ursprung der Hacker-aktivität im internen Netzwerk liegt. Geht es aus Angreifersicht um einen erfolgreichen Aufbau einer Remote-Control Verbindung, bedient man sich der sogenannten **Tunneling-Verfahren**. Diese benutzen ein Protokoll, um den Firewall zu umgehen. Typische Protokolle sind HTTP, Mail oder DNS.

Aus der Sicht von Compass Security sind solche **Inside-Out Tunneling Attacken** eine grosse Bedrohung. Der Fachwelt ist jedoch zuwenig bewusst, welches Potenzial solche Inside-Out Attacken haben. Im Rahmen dieser Arbeit wurde ein Windows Programm und ein Linux DNS-Tunnel Server realisiert. Über DNS-Anfragen baut das Windows Programm einen Tunnel zu dem im Internet stehenden DNS-Tunnel Server auf. Dieser Tunnel wird als Test-Case aufgebaut und lässt sich über eine Webseite steuern.

Damit steht erstmals im Internet ein Test-Tool zur Verfügung, das die Verwundbarkeit gegenüber einer DNS Tunnel Inside-Out Attacke testet. Der DNS Tunnel bietet folgende Funktionalität:

- Übertragung von Dateien vom DNS Tunnel Server zum Client
- Übertragung von Dateien vom Client zum DNS Tunnel Server
- Ausführen von Programmen auf dem Client

Vor der Implementation wurde analysiert, in welche Felder des DNS Protokolls eigene Daten gepackt werden können. Für die Übertragung vom Client zum Server besteht einzig die Möglichkeit, die Daten in dem Feld unterzubringen, das den Hostnamen enthält ("Query Name field"). Für die Datenübertragung vom Server zum Client wird ein Feld genutzt, das normalerweise eine Beschreibung zum DNS-Eintrag enthält ("TXT field").

Um einen maximalen Schutz gegenüber Missbrauch zu gewährleisten, wird bei der Ausführung des Client Tools eine Warnung ausgegeben, die der Benutzer bestätigen muss. Zudem ist die Internet Adresse des DNS Tunnel Servers im Client fest einkompiliert. Es ist eine wichtige Anforderung an diese Diplomarbeit, dass das Produkt als Instrument zur Security Sensibilisierung verwendet werden kann und als echtes Hacker-Tool versagt.