MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München
und Technische Universität München
Prof. Dr. H.-G. Hegering

Praktikum IT-Sicherheit
Übungsblatt 09

22. SOCKS

(a) Installieren Sie den Dante-Server und Client über `YaST2` auf Ihrer Maschine und lesen Sie die Man-Pages für die Konfigurationsfiles (`man sockd.conf` und `man socks.conf`).

(b) Sie arbeiten immer mit Ihrem Partnerrechner zusammen, d.h. Sie installieren und konfigurieren den Dante-Server auf Ihrem Rechner und den Dante-Client auf Ihrem Partnerrechner um darüber zu testen. Das schließt ein, dass Sie dafür Sorge zu tragen haben, dass die 'Besatzung' Ihres Partnerrechners die Möglichkeit hat, das Clientkonfigurationsfile `/etc/socks.conf` zu editieren.

(c) Erstellen Sie als Grundkonfiguration des Dante-Servers folgendes:

- Die Logfile-Einträge sollen nach `/var/log/messages` geschrieben werden.
- Das Logging jeder Regel soll maximal sein.
- Legen Sie die interne und externe IP-Adresse Ihres Dante-Servers fest.
- Legen Sie fest, dass für die Client-Regeln keine Authentisierung nötig ist.
- Editieren Sie Client-Regeln so, dass es grundsätzlich Ihrem Partnerrechner erlaubt ist, Sie als SOCKS-Server zu verwenden.
- Blocken Sie alle anderen Verbindungsaufbauversuche.
- Erlauben Sie folgendes bei den Serverregeln:
  - Niemand soll Ihr Loopback Interface erreichen dürfen.
  - Telnet und SSH soll von Ihrem Partnerrechner aus ins Netz `192.168.216.0/24` erlaubt sein, andere Ziele werden blockiert.
  - Telnet und SSH soll von Ihrem Partnerrechner aus in die Domäne '`.secp.nm.informatik.uni-muenchen.de`' erlaubt sein, andere Domänen sollen blockiert werden.
  - Alle anderen Verbindungen werden unterbunden.

(d) Konfigurieren Sie den Dante-Client Ihres Partnerrechners so, dass

- DNS-Auflösung über UDP funktioniert.
- der auf Ihrem Partnerrechner eingetragene Nameserver in der `/etc/resolv.conf` direkt und nicht über den SOCKS-Server angesprochen wird.
- Anfragen an das Loopback Interface Ihres Clients direkt gehen.
- Kommunikation zwischen Ihrem Rechner und Ihrem Partnerrechner direkt geht.
- alle andere Kommunikation (auf IP-Basis oder über Namen) an den Dante-Server geschickt wird.

(e) Prüfen Sie die Client- und Serverkonfiguration, indem Sie versuchen, Verbindungen über Telnet, SSH und z.B. HTTP zu den unterschiedlichsten Zielen aufzubauen. Dies geschieht z.B. bei Telnet mit `socksify telnet 192.168.216.254`. Treten Probleme auf, überprüfen Sie das Logfile Ihres Dante-Servers. Es kann auch der Debug-Level des Clients erhöht und die Logausgaben nach STDOUT gelenkt werden.

Für alle, die sich noch etwas mit dem Dante-Server spielen wollen, hier noch ein paar Zusatzaufgaben. Die Bearbeitung ist auf freiwilliger Basis:

(a) Wie ist die Konfiguration Ihres Servers und des Clients abzuändern, wenn der Client keine DNS-Auflösung besitzt und der Server diese übernimmt?

(b) Sie haben mehrere Nutzer auf dem Client, wollen aber nur einem bestimmten Nutzer den Zugriff auf eine spezielle Einstellung Ihres Servers erlauben (Authentisierungsmethode `username`). Wie realisieren Sie dies?