

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

Praktikum IT-Sicherheit
Übungsblatt 08

20. Squid

- (a) Deaktivieren Sie alle Paketfilterregeln und sorgen Sie dafür, dass alle Dienste auf allen Interfaces hören und von allen Adressen aus dem Netz 192.168.216.0/24 erreichbar und nutzbar sind.
- (b) Installieren Sie Squid von der SuSE DVD.
- (c) Tragen Sie in der `/etc/resolv.conf` den Rechner 192.168.216.254 als einzigen Nameserver ein.
- (d) Nun folgt die Squidkonfiguration: **Überprüfen Sie alle logischen Teilschritte mittels in der Vorbereitung beschriebener Tests und der Logfile-Einträge. Gehen Sie immer schrittweise vor!**
 - Setzen Sie den Squid Port auf 8888. Der ICP Port ist standardmäßig 3130.
 - Setzen Sie die bei einer Fehlermeldung angezeigte Mailadresse auf den `root`-Account Ihres Rechners.
 - Es sind nur anfragende Rechner aus den Domänen `.de` und `.org` erlaubt.
 - Bei allen Definitionen der übergeordneten Proxies soll dafür gesorgt werden, dass
 - kein von diesem Cache geholt Objekt gespeichert wird.
 - keine ICP-Anfrage erfolgt.Alle übergeordneten Proxies sind als `parent` zu betrachten.

- Implementieren Sie ein Proxychaining, dass hier beispielhaft für `pcsec04` und `pcsec03` dargestellt ist. Bitte transferieren Sie die hier gemachten Angaben auf Ihre spezielle Situation:
 - Proxychain für `pcsec04`:
 - * `pcsec04.secp.nm.informatik.uni-muenchen.de` und `pcsec03.secp.nm.informatik.uni-muenchen.de` sind lokal aufzulösen. Hierzu ist keine Nutzer-Authentisierung nötig.
 - * Schicken Sie alle anderen Anfragen an den in der Hierarchie über Ihnen stehenden Cache `pcsec03 192.168.216.23`.
 - * Erlauben Sie nur Ihrem Rechner und dem Rechner `pcsec03`, Ihren Cache zu verwenden.
 - * Laden Sie sich aus dem Internet den aktuellen Squid-Quellcode herunter und entpacken Sie ihn. Installieren Sie das Authentisierungsprogramm `ncsa_auth`, erzeugen Sie ein Authentisierungsfile mit `htpasswd` und aktivieren Sie die Authentisierung in der `/etc/squid.conf`.
 - * Erlauben Sie alle URLs in der Domain `secp.nm.informatik.uni-muenchen.de` ohne Authentisierung.
 - * Verlangen Sie für alle restlichen Verbindungen in den erlaubten Domains `.de` und `.org` Authentisierung.
 - Proxychain für `pcsec03`:
 - * `pcsec04.secp.nm.informatik.uni-muenchen.de` und `pcsec03.secp.nm.informatik.uni-muenchen.de` sind lokal aufzulösen. Hierzu ist keine Userauthentisierung nötig.
 - * Schicken Sie alle anderen Anfragen an den in der Hierarchie über Ihnen stehenden Cache `secserver 192.168.216.254` HTTP Port 3128, ICP Port 3130. Dabei müssen Sie bedenken, dass zumindest der `secserver` für den Zugriff auf die von Ihnen direkt aufzulösenden Domains erlaubt sein muss.
 - * Sorgen Sie dafür, dass alle Rechner mit ungerader Nummer nur die Webseiten `pcsec04.secp.nm.informatik.uni-muenchen.de` und `pcsec03.secp.nm.informatik.uni-muenchen.de` über Ihren Cache erreichen können.

* Sorgen Sie dafür, dass `pcsec04` und Ihr Rechner alle erlaubten Domains ohne Userauthentisierung erreichen können.

21. GnuPG

- (a) Installieren Sie GnuPG auf Ihrer Maschine, sofern es nicht schon vorhanden ist.
- (b) Erzeugen Sie sich ein neues Schlüsselpaar und schützen Sie den privaten Schlüssel mit einem starken Mantra.
- (c) Exportieren Sie Ihren öffentlichen Schlüssel und machen Sie ihn Ihrem Partner zugänglich.
- (d) Importieren Sie den Schlüssel Ihres Partners in Ihren Schlüsselbund.
- (e) Schicken Sie ihrem Partner eine
 - verschlüsselte und signierte Nachricht.
 - eine Nachricht im Klartext mit Signatur.
 - eine Nachricht im Klartext und Signatur in einer separaten Datei.
- (f) Entschlüsseln bzw. verifizieren Sie die erhaltenen Nachrichten.
- (g) Signieren Sie den Schlüssel ihres Partners.
- (h) Erstellen Sie ein Schlüsselwiderruf-Zertifikat für Ihren Schlüssel.