Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2009/2010
Übungsblatt 10

Abgabetermin: 03.02.2010 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 23: (H) TLS/SSLv3 Renegotiation Vulnerability

In der Vorlesung wurden die Themen Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS) erläutert.

a. Beschreiben Sie die SSL/TLS Protokoll-Architektur und stichpunktartig die Aufgaben des jeweiligen Protokolls

b. Die in der Vorlesung für HTTPS vorgestellte Renegotiation Vulnerability, die im November 2009 bekannt wurde, betrifft auch weitere Protokolle, wie z.B. SMTP. Skizzieren Sie den Ablauf für eine SMTP over TLS (STARTSSL). Gehen Sie davon aus, dass der Angreifer auf dem Mailserver einen Account besitzt.

c. Welche Voraussetzungen sind für diese Renegotiation-Angriffe generell notwendig? Welche Voraussetzung gilt im Speziellen bei dem SMTP-Szenario?

d. Welche wirkungsvollen Gegenmaßnahmen kann man treffen?

Aufgabe 24: (H) Methoden zur Spam-Bekämpfung

Es existieren verschiedene Methoden, die Spammer unter anderem nutzen:

- Non-Primary MX attack
- Spam troll / Dictionary attack
- Organized distributed attack

a. Erläutern Sie stichpunktartig die Methoden “Non-Primary MX attack” und “Spam troll/Dictionary attack”.

b. Zur Spam-Abwehr werden verschiedene Methoden eingesetzt. Beschreiben Sie das Greylisting-Verfahren und wie Greylisting auf die oben genannten Angriffsmethoden reagiert.

Ein neueres Verfahren zur SPAM-Bekämpfung ist Hashcash

a. Erläutern Sie kurz dieses Verfahren

b. Besitzt dieses Verfahren negative Auswirkungen auf den Versand regulärer E-Mail-Nachrichten?

c. Ab Version 3.0 unterstützt das Tool SpamAssassin das HashCash-Verfahren. Wie sieht eine mögliche Konfiguration aus, die für alle Nutzer der Domain “@campus.lmu.de” das HashCash-Verfahren verwendet? Beschränken Sie sich hier auf den HashCash-Abschnitt.