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 2011/2012
Übungsblatt 3

Abgabetermin: 16.11.2011 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 **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich 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 7: (H) Security Engineering

Das Security Engineering ist eines der zentralen Themen in der IT-Sicherheit. Das Ziel, das dabei grundsätzlich verfolgt wird, ist die Konstruktion sicherer IT-Systeme und -Infrastrukturen.

a. Nennen und erläutern Sie mindestens 4 Gründe, warum sich die Methoden für die Konstruktion sicherer Systeme kaum entwickelt haben.

b. Das Thema *Sicherheit* sollte von Anfang an in dem Entwicklungsprozess berücksichtigt werden. Im Security Engineering existieren an dieser Stelle eine Reihe von Prinzipien:

   - Prinzip der minimalen Rechte (Least privileges)
   - Verbote sind Standard (Fail-Safe default)
   - Sicherheit hängt nicht von Geheimhaltung ab (Open design)
   - Trennung von Rechten (Separation of duties)

   Erläutern Sie diese vier hier genannten Prinzipien und geben Sie jeweils ein Beispiel an.

c. Im Security Engineering werden Design Patterns, die funktionale Aspekte des Systems beschreiben, um Security Patterns ergänzt. Diese lassen sich über die Begriffe *Kontext*, *Problem und Bedrohungen*, *Sicherheitsanforderungen*, *Lösung* beschreiben. Der Kontext für die Verwendung von Cookies könnte wie folgt lauten: *Cookies werden zum Speichern und Abfragen von Nutzerinformationen verwendet und im Allgemeinen von Servern beim Benutzer platziert*. Ergänzen Sie das zugehörige Security Pattern.

Aufgabe 8: (H) Angreifermodell, Angriffsarten, External SSH-Scans

In der Vorlesung wurden verschiedende Aspekte im Zusammenhang mit Bedrohungen und Angriffen auf IT-Infrastrukturen vorgestellt.

a. Begründen Sie, warum eine im Rahmen von ISO/IEC 27001 durchgeführte Risikobewertung sehr stark vom Angreifermodell abhängt.

b. Es existieren verschiedene Angriffsarten (aktiv, passiv, Social Engineering). Erläutern Sie diese und geben Sie jeweils einen konkreten Beispielangriff an.

c. Weltweit erreichbare Systeme im Münchner Wissenschaftsnetz sind tagtäglich SSH-Scan-Angriffen ausgesetzt, die in Verbindung mit einer Wörterbuchattacke versuchen, schwache Passwörter zu brechen, um unberechtigten Zugang zu dem System zu erhalten. Zum Schutz der Systeme haben sich Werkzeuge wie *Denyhosts* bewährt. Laden sie sich dieses Werkzeug aus dem Internet herunter und definieren Sie die entsprechenden Parameter in der Konfigurationsdatei *denyhosts.cfg*

   – Die Datei /var/log/messages soll überwacht werden
   – Schwellwert invalider Logins, z.B. nicht existente Loginnamen, soll den Wert 3 besitzen
   – Schwellwert bei Verwendung gültiger Loginnamen, soll den Wert 7 besitzen
   – Geblockte IP-Adressen sollen nach 2 Stunden automatisch freigeschaltet werden

   Fügen Sie die eingestellten Parameter Ihrer Hausaufgabe hinzu.