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 1

Abgabetermin: 02.11.2011 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 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 1: (H) Ziele der Informationssicherheit & wichtige Begriffe

In der Vorlesung wurden Ihnen Grundlagen und wichtige Begriffe im Bereich der Informationssicherheit erläutert.

a. Nennen Sie die mindestens 8 Ziele (Schutzziele), die im Allgemeinen im IT-Sicherheitsumfeld relevant sind. Erläutern Sie diese Ziele knapp und nennen Sie mindestens einen Mechanismus oder eine Methode, um dieses Ziel zu erreichen. Geben Sie auch ein Beispiel oder eine Erklärung an, in welchem Fall das jeweilige Schutzziel verletzt ist.

b. Erläutern Sie die Begriffe *security*, *safety*, *protection* und *privacy*. Führen Sie, falls notwendig, auch eine Abgrenzung dieser Begriffe voneinander durch.

Aufgabe 2: (H) Botnetze

Eine der größten Bedrohungen, denen Unternehmen und deren IT-Infrastruktur heutzutage ausgesetzt sind, stellen sog. Botnetze dar.

a. Definieren Sie kurz den Begriff *Botnetz*. Nennen Sie wichtige Komponenten und beschreiben Sie knapp deren Funktion. Erläutern Sie die grundsätzliche Funktionsweise und nennen Sie einen Einsatzzweck eines Botnetzes.

b. Command & Control Server (CC-Server) werden im Allgemeinen zur Steuerung der Botnet-Clients eingesetzt. Nennen und beschreiben Sie stichpunktartig mindestens drei Varianten für die Kommunikation zwischen CC-Server und Client.

c. Was versteht man unter dem Begriff *Fast Flux/Fast Flux Netzwerk*? Welche Rolle spielt dieser im Zusammenhang mit Botnetzen?

Aufgabe 3: (T) TDL-4 - Das nahezu unzerstörbare Botnetz

Ein im Augenblick sehr bekanntes und überaus gefährliches Botnetz ist das TDL-4-Botnetz. Sicherheitsexperten waren sich Ende Juni 2011 einig, dass es als nahezu unzerstörbar anzusehen ist. Unter anderem werden in dieser Aufgabe Verbreitungswege, die Infektion des Endsystems mit dem Rootkit, als auch einige Schutzmechanismen des Schadprogramms vorgestellt.