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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2016/2017
Übungsblatt 4

Termin: 29.11.2016 um 12:00 Uhr

Aufgabe 7: (K) Malicious Code & SPAM-Protection

a. Zur Erkennung von Malicious Code auf einem System werden in der Regel Antiviren-Programme eingesetzt, die eine Reihe verschiedener Erkennungstechniken kombiniert verwenden. Erläutern Sie *Signatur-basierte*, *Heuristische/Anomalie-basierte* und *Emulations-basierte Erkennung* und beschreiben sie jeweils die Stärken und Schwächen des jeweiligen Ansatzes.

b. Um der Erkennung durch aktuelle Antiviren-Programme zu entgehen, werden bei der Erstellung und Programmierung polymorpher Viren verschiedene Techniken eingesetzt. Erläutern Sie die folgenden Techniken

   - Garbage instructions
   - Instruction reordering
   - Interchangeable instructions

c. Es existieren verschiedene Maßnahmen, SPAM zu erkennen und diesen herauszufiltern bzw. zu blocken. Erläutern Sie folgende Verfahren: *DNS-basierte Blacklists*, *RHSBLs* und *naive Bayes-Klassifizierung*. Gehen Sie hier zusätzlich auf rechtliche Probleme ein, die Ihnen bei Einsatz dieser Verfahren begegnen.

d. Eine weitere Methode, neben dem in der Vorlesung vorgestellten Greylisting, zur Bekämpfung von SPAM ist Sender-Policy-Framework (SPF). Beschreiben Sie kurz die Funktionsweise und nennen Sie Vor- und Nachteile gegenüber Greylisting.

Aufgabe 8: (K) Buffer-Overflow

Angreifer nutzen oftmals Schwachstellen in lokal installierten Applikationen.

a. Erläutern Sie, was bei einem Buffer-Overflow genau passiert und wie ein Angreifer diesen für einen Angriff ausnutzen könnte?

b. Beschreiben Sie den Unterschied zwischen einem klassischen Buffer-Overflow und einem return-to-libc Angriff.

c. Nennen und beschreiben Sie mindestens drei Schutzmaßnahmen, die zum Schutz vor Buffer-Overflows eingesetzt werden können.