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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2014/2015
Übungsblatt 3

Abgabetermin: 11.11.2014 bis 12:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als Einzelabgabe). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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 5: **(H)** DoS & DDoS (6 Punkte)

In der Vorlesung wurden verschiedende Angriffstechniken vorgestellt, u.a. auch DoS und DDoS-Attacken.

a. Erläutern Sie den grundsätzlichen Ablauf eines DDoS-Angriffs. Welche wirksamen Gegenmaßnahmen sehen Sie?

b. DDoS-Angriffe gehen meist von zu einem Botnet zusammengeschlossenen, Malware-infizierten Systemen aus. Bei der Kommunikation der Zombie-Systeme mit ihrem Command-and-Control-Server (CnC) unterscheidet man zwischen Star-, Multi-Server-, Hierarchical- und Random. Erläutern Sie in Stichpunkten diese Kommunikationsarten. Welche Vor- bzw. Nachteile ergeben sich aus der jeweiligen Art für die Zerstörung des Botnetzes?

c. In der Vorlesung wurde der Ablauf eines DNS-Amplification Angriffs erläutert. Die unter CVE-2013-5211 bekannte Schwachstelle ermöglicht einen ähnlichen Angriff auf NTP-Server. Erläutern Sie den Ablauf einer darauf basierenden NTP-Amplification Attack.

d. Als wirksame Gegenmaßnahme für einen Syn-Flooding-Angriff wurden im Rahmen der Vorlesung Syn-Cookies erläutert. Weitere Gegenmaßnahmen sind RST-Cookies, Micro Blocks und Stack Tweaking. Erläutern Sie diese kurz.

Aufgabe 6: (H) Malicious Code & SPAM-Protection (8 Punkte)

Tagtäglich gibt es Meldungen über die Ausbreitung von Malicious Code. Unter diesem Sammelbegriff werden im Allgemeinen Schadprogramme wie Computerviren, -würmer und Trojanische Pferde verstanden.

a. Zur Erkennung von Malicious Code auf einem System werden in der Regel Anti-Virus-Programme eingesetzt, die eine Reihe von Erkennungstechniken kombiniert verwenden. Erläutern Sie *Signatur-basierte*, *Heuristische/Anomalie-basierte* und *Emulations-basierte Erkennung*.

b. Welche Stärken bzw. Schwächen weisen die in der vorherigen Teilaufgabe beschriebenen Erkennungstechniken auf? Welche logische Schlussfolgerung ergibt sich daraus für die Hersteller von Anti-Virensoftware?

c. Um der Erkennung durch aktuelle Anti-Viren-Programme zu entgehen, werden bei der Programmierung insbesondere polymorpher Viren verschiedene Techniken eingesetzt. Erläutern Sie die Methoden

   - Garbage instructions
   - Instruction reordering
   - Interchangeable instructions

d. Der Versand von SPAM, welcher oftmals auf eine Infektion eines Systems mit einem Schadprogramm zurückzuführen ist, ist seit einigen Jahren ein großes Problem. 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*. Welche rechtlichen Probleme könnten beim Einsatz DNS-basierter Blacklists bestehen?

Aufgabe 7: (H) CVE-2012-2122: Vulnerable MySQL-Servers (2 Punkte)

Ein befreundeter Hacker erzählt Ihnen, dass sich auf dem System mit der IP-Adresse 2331380773 ein für CVE-2012-2122 verwundbarer MySQL-Server befindet. Nutzen Sie die Lücke aus. Welche Datenbanken und Tabellen existieren dort und welche Nutzer sind zugriffsberechtigt? (Hinweis: Verbinden Sie sich bei unerwarteten Verbindungsabbrüchen ggf. mehrfach mit der Datenbank!)