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 2017/2018
Übungsblatt 2

Abgabetermin: 14.11.2017 um 12:00 Uhr

Aufgabe 4: (K) DoS & DDoS

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

a. Erläutern Sie in Stichpunkten den Ablauf von DoS- und DDoS-Angriffen und zeigen Sie wirksame Gegenmaßnahmen auf.

b. Erläutern Sie konkret die Funktionsweise von Syn-Cookies und zeigen Sie, wie dadurch Syn-Flooding Attacken vermieden werden können!

c. Welche Nachteile haben Syn-Cookies?

Aufgabe 5: (K) Worms & Trojans

Suart Stainford, Vern Paxson und Nicholas Weaver beschreiben in ihrem Artikel (`http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf`) verschiedene Ausbeitungsarten von Würmern.

a. Erläutern Sie *Random Scanning*, *Permutation Scanning*, *Hit-List Scanning* und *Topological Scanning*. Geben Sie zusätzlich die Vor- bzw. Nachteile der jeweiligen Strategie an.

b. Was versteht man unter dem Begriff *Warhol Worm*? Wodurch erreicht dieses Konzept seine hohe Ausbreitungsgeschwindigkeit?

c. Erläutern Sie den Zusammenhang oder Unterschied zwischen einem Trojanischen Pferd und

   - einer Backdoor
   - mobile Code