

IT-Sicherheit im Wintersemester 2018/2019

Übungsblatt 2

Termin: 06.11.2018 um 12:00 Uhr

Aufgabe 4: (K) DoS & DDoS

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

- Erläutern Sie in Stichpunkten den Ablauf von DoS- und DDoS-Angriffen und zeigen Sie wirksame Gegenmaßnahmen auf.
- Erläutern Sie konkret die Funktionsweise von Syn-Cookies und zeigen Sie, wie dadurch Syn-Flooding Attacken vermieden werden können!
- Welche Nachteile haben Syn-Cookies?
- Neben SYN-Cookies existieren auch sog. RST-Cookies. Beschreiben Sie deren Funktionsweise.

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 Ausbreitungsarten von Würmern.

- Erläutern Sie *Random Scanning*, *Permutation Scanning*, *Hit-List Scanning* und *Topological Scanning*. Geben Sie zusätzlich die Vor- bzw. Nachteile der jeweiligen Strategie an.
- Was versteht man unter dem Begriff *Warhol Worm*? Wodurch erreicht dieses Konzept seine hohe Ausbreitungsgeschwindigkeit?
- Erläutern Sie den Zusammenhang oder Unterschied zwischen einem Trojanischen Pferd und
 - einer Backdoor
 - mobile Code