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 2024/2025
Übungsblatt 2

Besprechung: Do, 07.11.2024

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

Aufgabe 1: (T) DoS & DDoS

In der Vorlesung wurden verschiedene 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?

d. Neben SYN-Cookies existieren auch sog. RST-Cookies. Beschreiben Sie deren Funktionsweise.

Aufgabe 2: (T) Ransomware und WannaCry

WannaCry ist ein bekannter Vertreter der Ransomware-Gattung, die weitreichenden Schaden bei Opfern anrichten kann.

a. Nach welchem Grundprinzip arbeitet Ransomware? Welche Ziele werden damit verfolgt?

b. Wie lassen sich von Ransomware betroffene Systeme wiederherstellen? Sollte das Lösegeld (Ransom) gezahlt werden?

c. Wie kann sich gegen Ransomware geschützt werden?

d. Wie breitete sich WannaCry aus? Was stoppte deren Ausbreitung?

Aufgabe 3: (T) NTP, Amplification & NTS

Das *Network Time Protocol* (NTP) von 1985 (v3: RFC1305, 1992; v4: RFC5905, 2010) dient zur Synchronisierung von Uhren über Kommunikationsnetze. Es ist eines der wenigen ungesicherten und nicht authentifizierten Internetprotokolle, das noch immer weit verbreitet ist.

a. Warum wird eine (präzise) Uhrensynchronisierung in Kommunikationssystemen benötigt?

b. Welche Probleme könnten sich ergeben, wenn es einem Angreifer gelingt, die Uhren seines Opfers zu manipulieren?

c. Welche Arten von Angriffen auf bzw. über das *Network Time Protocol* sind denkbar?

d. Was wird unter Amplification-Attacks verstanden? Wie funktioniert eine NTP-Amplification und worauf zielt diese ab?

e. Wie lassen sich NTP-Amplification-Attacks verhindern? Welche Rolle kann der NTP-Nachfolger *Network Time Security* (NTS) dabei spielen?

Aufgabe 4: (H) Worms & Trojans

Suart Stainford, Vern Paxson und Nicholas Weaver beschreiben in ihrem Artikel (`https://web.archive.org/web/20240719080842/https://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf`) verschiedene Ausbreitungsarten 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 wird unter dem Begriff *Warhol Worm* verstanden? Wodurch erreicht dieses Konzept dessen hohe Ausbreitungsgeschwindigkeit?

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

   – einer Backdoor
   – mobile Code