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 5

**Termin:** 06.12.2016 um 12:00 Uhr

## Aufgabe 9: (K) Rootkits

Nachdem ein Angreifer erfolgreich Zugang zu einem IT-System, etwa durch das Ausnutzen einer dort vorhandenen Schwachstelle, erlangen konnte, wird dort meist ein Rootkit installiert.

a. Man unterscheidet grundsätzlich zwei Varianten von Rootkits: User-Mode- und Kernel-Mode-Rootkits. Erläutern Sie diese kurz.

b. Wie unterscheidet sich ein Rootkit von anderer Malware, z.B. Viren, Würmer und Trojanischen Pferden?

c. Rootkits verfügen im Allgemeinen über eine sogenannte *Dropper*-Komponente. Welchem Zweck dient diese Komponente. Was versteht man unter einem *Multistage Dropper*?

d. Charakteristisch für Rootkits sind sogenannte Anti-Forensik-Maßnahmen. Erläutern Sie folgende Maßnahmen

   - Data Destruction
   - Data Concealment
   - Data Fabrication

## Aufgabe 10: (K) Common Vulnerability Scoring System 3 (CVSSv3)

Für diese Aufgabe soll die folgende Schwachstellenbeschreibung verwendet werden, die über die vier Teilaufgaben hinweg modifiziert wird. Änderungen in einer der Teilaufgaben gelten auch in den darauf folgenden Teilaufgaben. (d.h. Änderungen in Teilaufgabe b) gelten auch für Teilaufgaben c) und d)).

*In einer weit verbreiteten Webanwendung, die in ihrem Unternehmen als Kundenportal zur Verwaltung von Softwarelizenzen verwendet wird und daher öffentlich im Internet zugänglich sein muss, existiert eine cross-site request forgery (CSRF) Schwachstelle. Durch diese Schwachstelle können Angreifer aus der Ferne Aktionen mit den Rechten des angegriffenen Benutzers ausführen, wenn der Benutzer eine aktive Session hat und dazu gebracht werden kann, einen schädlichen Link zu öffnen.*

Hinweis: Geben Sie bei den Aufgaben, bei denen explizit CVSS-Berechnungen gefordert sind, nicht nur deren Ergebnisse an, sondern begründen Sie auch die von Ihnen gewählten Optionen.

a. Beschreiben Sie kurz wie ein Angriff per CSRF üblicherweise funktioniert.

b. Berechnen Sie mithilfe des unter `https://www.first.org/cvss/calculator/3.0` verfügbaren CVSSv3-Calculators für die beschriebene Schwachstelle den CVSSv3 Base-Score. Vergleichen Sie diesen mit dem über `https://nvd.nist.gov/cvss.cfm?calculator&version=2` berechneten CVSSv2 Base-Score.

c. Die beschriebene Schwachstelle wurde am selben Tag auch auf der Security-Mailingliste *Full-Disclosure* publiziert und deren Ausnutzbarkeit anhand eines Proof-of-Concept (POC) bewiesen. Der Hersteller der Webanwendung hat die Schwachstelle nun auch offiziell bestätigt, aber bislang nur einen Workaround veröffentlicht. Wie verändert sich dadurch der CVSSv3 Base- bzw. Temporal-Score?

d. Bereits am nächsten Tag tauchte in einschlägigen Foren ein Exploit für diese Schwachstelle auf. Dieser besitzt keine besonderen Voraussetzungen und ist somit in jeder Situation funktional. Wie verändert sich dadurch der CVSSv3 Base-/Temporal-Score aus Aufgabe c)?

## Aufgabe 11: **(K)** Social Engineering

In der Vorlesung wurde ausführlich das Thema *Social Engineering* vorgestellt.

a. Nennen und erläutern Sie Kriterien bzw. leiten Sie daraus Kategorien ab, in die sich Social Engineering Angriffe sinnvoll einteilen lassen.

b. Als wirkungsvollste Maßnahme gegen Social Engineering Angriffen gilt nach wie vor, Mitarbeiter zu sensiblisieren und der Aufbau eines Security Awareness Programms. In der vom SANS-Institut herausgegebenen *Top 20 Security Controls* Liste wird auch das Control *Security Skills Assessment and Appropriate Training to Fill Gaps* angeführt. Nennen und erläutern Sie die insgesamt fünf wichtigen Aspekte, diese Maßnahme erfolgreich umzusetzen.