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 2015/2016
Übungsblatt 3

Abgabetermin: 10.11.2015 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**). Am Ende 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.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte an die Übungsleitung unter der E-Mail **uebung-itsec@lrz.de**.

Aufgabe 6: **(H)** Malicious Code (12 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 Antivirus-Programme eingesetzt, die eine Reihe von Erkennungstechniken kombiniert verwenden. Erläutern Sie *Signatur-basierte*, *Heuristische/Anomalie-basierte* und *Emulations-basierte Erkennung* und beschreiben sie jeweils die Stärken und Schwächen des Ansatzes.

b. Zur Erkennung und Analyse von Malicious Code werden häufig virtualisierte oder emulierte Umgebungen (z.B. Google Bouncer) verwendet. Aktuelle Schadsoftware ist in der Lage, herauszufinden, ob sie gerade getestet wird oder nicht. Nennen und erläutern Sie dazu drei verschiedene Methoden. (Siehe z.B. [1], [2])

c. Um der Erkennung durch aktuelle Antiviren-Programme zu entgehen, werden bei der Erstellung und Programmierung polymorpher Viren verschiedene Techniken eingesetzt. Erläutern Sie die folgenden Techniken

   - Garbage instructions
   - Instruction reordering

[1] http://www.simonganiere.ch/2012/11/20/malware-anti-vm-technics/
[2] http://static.usenix.org/event/woot09/tech/full_papers/paleari.pdf

- Interchangeable instructions

Aufgabe 7: **(H)** Worms & Trojans (8 Punkte)

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.

Aufgabe 8: **(K)** Antivirus im Unternehmen

Versetzen Sie sich in die Lage eines Informationssicherheitsverantwortlichen, den die Unternehmenleitung beauftragt, sich eine Scan-Policy für die auf den Windows-basierten Arbeitsplatzsystemen installierte Antiviren-Software zu überlegen. Erstellen Sie exemplarisch eine solche Policy und berücksichtigen dabei u.a. folgende Randbedingungen:

- On-Demand-Scanning
- On-Access-Scanning (Echtzeit-Überprüfung von Lese- und Schreibzugriffen)
- Definition expliziter Ausnahmen von diesen beiden Scanning-Varianten
- Regelmäßige Updates der Software und insbesondere der Signaturen
- Geringe Auswirkungen auf die System-Performanz
- ...

Aufgabe 9: **(T)** Der Wirtschaftssektor Malware-Verbreitung

Anfangs standen alleinig die Beschäftigung mit der Technik und das Kennenlernen und Ausreizen von Möglichkeiten, welche Computersysteme zum damaligen Zeitpunkt boten, im Vordergrund. Im Laufe der Zeit spielten aber eher auch Anerkennung in Hackerkreisen eine Rolle. Seit einigen Jahren ist jedoch eine Kriminalisierung dieser Szene beobachtbar, so dass finanzielle Interessen in den Vordergrund gerückt sind. In dieser Aufgabe soll ein kurzer Einblick in diesen Wandel gegeben werden. U.a. geht es hierbei um um heutige Verbreitungswege der Malware.