Reaktive Sicherheit

Übungsblatt 8

Balduin Binder [s6babind@uni-bonn.de] Charlotte Mädler [s6chmaed@uni-bonn.de]
Bünyamin Sarikaya [s6busari@uni-bonn.de]

Aufgabe 2

(1) FakeNet: simuliert ein Netzwerk wobei jeglicher Netzwerkverkehr an localhost weitergeleitet wird, wodurch keine Daten nach außen gehen können. So kann man Schadsoftware analysieren (Verhalten, etc.).

RegShot: (RegistryShot) ermöglicht es Snapshots von Registries zu machen. Dies ist nützlich um den genauen Ablauf/Verhalten von Schadsoftware weiter zu analysieren.

Process Monitor: zeichnet alle TCP/IP-Verbindungen auf, wie auch Lese- und Schreibzugriffe auf das Dateiensystem und Registry.

Process Explorer: gibt ein Überblick über alle derzeitig laufende Prozesse, geladene Dateien und Speciehrzugriffe.

strings2 : extrahiert Unicode (und ASCII) Strings aus Binärdateien.

YaraGUI: ist eine Benutzeroberfläche zum Malware identifizieren.

Wireshark: stellt den Netzwerkverkehr da

(2)

(3)

Aufgabe 4

(3)

(4)

(5)

(6)