HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Studenten	**Fernando Garcia** **Flavio Grisch**
Titel der Studienarbeit	**Honeynet**
Examinatorin / Examinator	**Prof. Dr. Peter Heinzmann** **Dipl. Ing. Marcel Liebi**

Kurzfassung der Studienarbeit

Honeypots, auch Decoy IDS genannt, werden in der IT-Security zur Analyse von Angriffen in Netzwerken, zur Abschreckung von potentiellen Eindringlingen und zur Gewinnung neuer Erkenntnisse der installierten Sicherheitskomponenten eingesetzt. Honeynets sind mehrere solcher Honeypots, welche zu einem Netzwerk zusammengeschlossen werden. Sie dienen hauptsächlich der Analyse von Angriffen.

Im Rahmen dieser Studienarbeit wurde die Thematik Honeypot/Honeynet ausführlich behandelt, ein Lab über Honeypots zusammengestellt und den Aufbau eines Home Made Honeypots erarbeitet.

- Das Lab zeigt die Zusammenarbeit zwischen dem Honeypot Honeyd und dem dazu notwendigen Tool Arpd. Honeyd ist ein Low-Interactive-Honeypot, welcher in erster Linie Services emuliert und in zweiter Linie Angriffe loggt. Arpd ist ein Tool auf Basis von ARP, welches alle ungenutzten IP's auf einem Netzwerk auf einen Rechner bindet. Scans und Probes werden so auf den Honeypot geleitet.

- Der Home Made Honeypot ist ein Beispiel wie man einen Honeypot mit voneinander unabhängigen Open Source Tools aufbauen kann. Es werden HIDS, NIDS, Logger und Analyse Tools verwendet, welche alle Informationen zu einer Attacke für eine spätere Analyse aufzeichnen.

Des Weiteren wurde ein vertiefter Einblick in die recht junge Thematik Honeypot/Honeynet verschafft, um die teils recht unterschiedlichen Ansichten und Definitionen zu überblicken, zu analysieren und in einem Bericht zu verfassen.