Honeynets und Honeypots

Von

Doris Reim

24.02.2007

Seminar: Internet Sicherheit

Lehrstuhl: INET

TU Berlin

Einleitung

- Begrenzte Möglichkeiten mit Intrusion Detection Systemen, Antivirensoftware und Firewalls
- Automatisierte Angriffe
- Alternativer Ansatz Honeynets:
  - Scriptkiddies mit scheinbar unsicheren Systemen ködern
  - Möglichkeit der Forensik (Offline-Analyse des Systems)

Inhalt

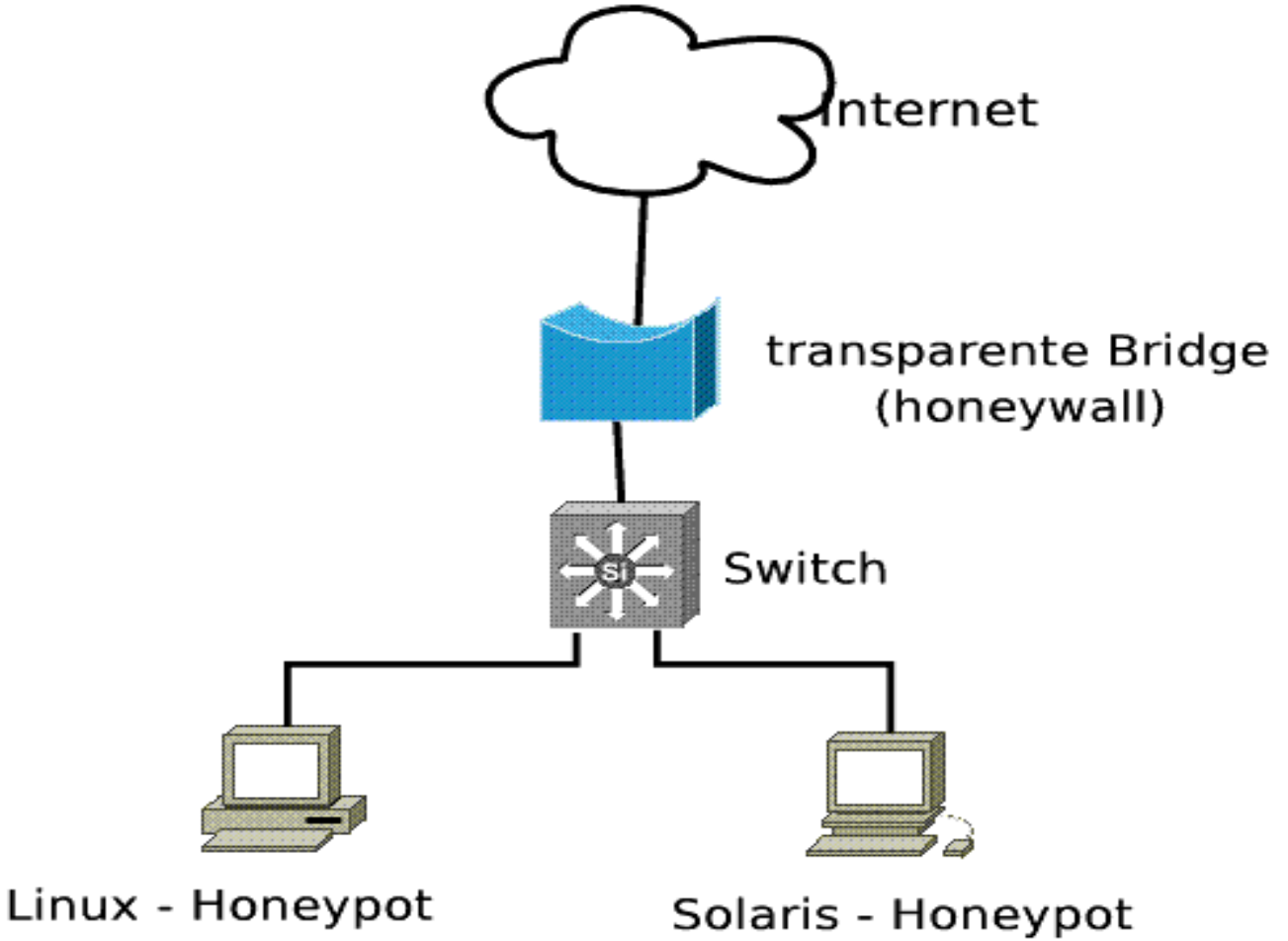
Honeynet und Honeypot

- Honeypot:
  - „normaler“ Rechner, der verschiedene Dienste im Netz anbietet, z.B. FTP
  - Ausgerüstet mit spezieller Software:
    - Daten sammeln
    - Unerkannt bleiben
  - Zusätzlich transparente Bridge - Honeywall:
    - Schützt das Netz vor dem Honeypot: verhindert Angriffe vom Honeypot aus auf andere Systeme
    - Muß unsichtbar bleiben

Honeynet und Honeypot

- Honeynet:
  - Zusammenschluß mehrerer Honypots zu einem Netz
  - Vorteile:
    - Verschiedene Betriebssysteme
    - Verschiedene Dienste auf verschiedenen Systemen
  - Virtuelle Honeynets: mehrere virtuelle BS auf einem System

Beispieltopologie



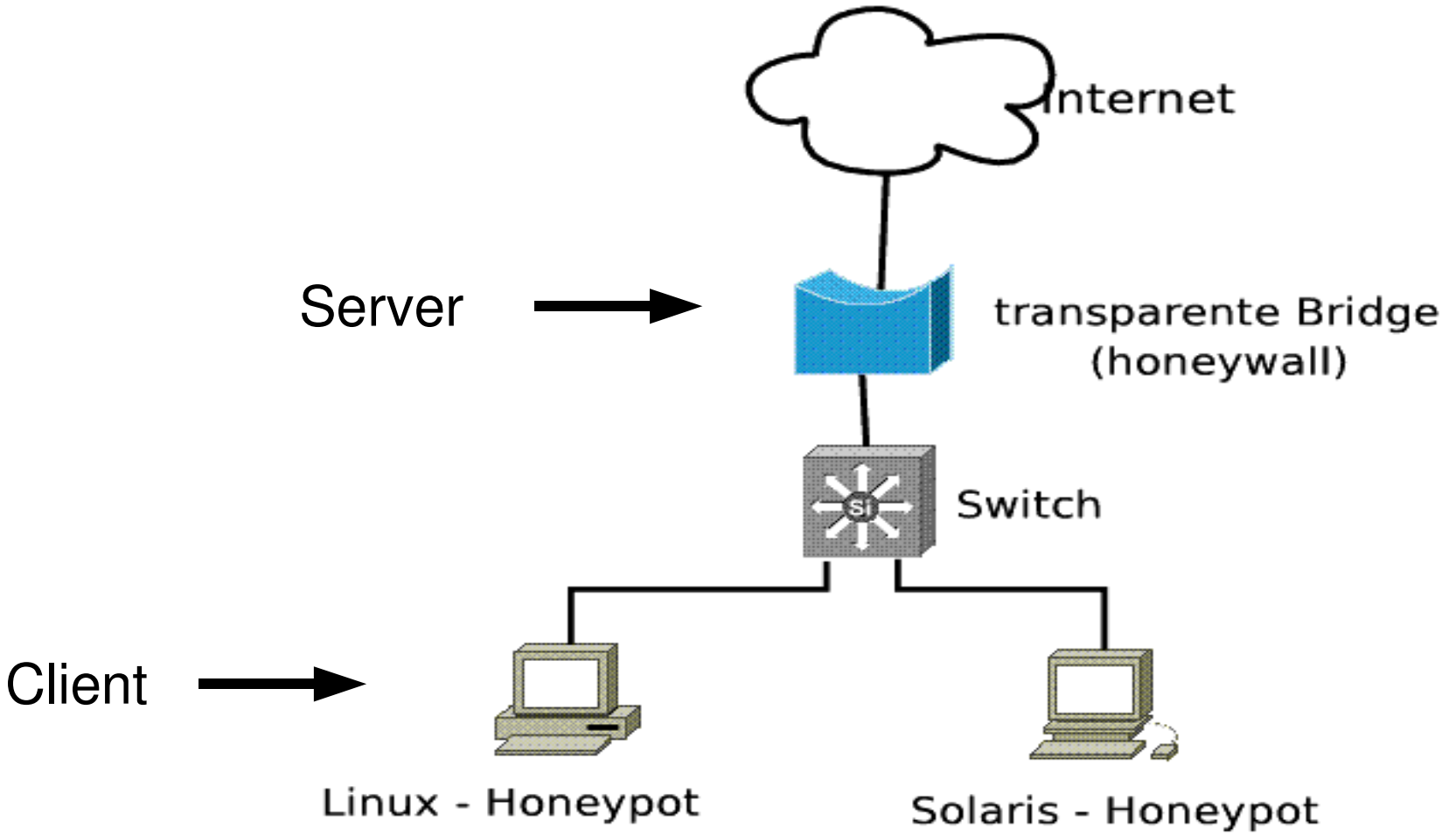
Das Honeynet Project

- www.honeynet.org
- Zusammenschluß von (Forschungs-) Gruppen und Einzelpersonen
- Informationen und Software zu den Themen Angriffe auf Rechner, Schutzmaßnahmen und speziell zu Honeynets

Die Werkzeuge

- Sebek:
  - Client:
    - Auf dem Honeypot installiert
    - Sammelt Daten und versendet diese an den Server
  - Server:
    - Oft auf der Honeywall installiert
    - Sammelt Daten der Honeypots
- Weitere Tools zur Analyse: z.B. tcpdump, traceroute, Honeysnap...

Beispieltopologie



Inhalt

Honeynets an Hochschulen

- Vorteile:
  - Forschung: Sammlung großer Datenmengen
  - Lehre: kann auf realen Daten aufbauen
  - Sicherheit: Honeynets als zusätzliches Sicherheitswerkzeug
- Vorarbeiten:
  - Information:
    - Was wird benötigt?
    - Gefahren
  - Überzeugungsarbeit: Bei der Hochschulleitung und den Administratoren

Honeynets an Hochschulen

- Kosten
  - Hardware: keine aufwendige Hardware nötig 
  - Software: als Open Source verfügbar 
- Der Anfang
  - Möglichst einfache Topologie
  - Möglichst einfache Konfiguration des Systems
- Weiterentwicklung:
  - Komplexität erhöhen
  - Bekanntes real einsetzen (siehe folgendes Kapitel)

Inhalt

RWTH Aachen

- Aufbau:
  - Eigenes /26-Netz, abgeschirmt vom Universitätsnetz
  - 2 Honeypots (Solaris und Suse Linux) hinter Honeywall
  - Linux: 3 Benutzer, Köderdaten, HTTP, FTP und SSH
- Ergebnisse zwischen 2003 und 2004:
  - Keine Kompromittierung, aber viele port scans registriert
  - Selbst Methode entdeckt, Sebek aufzuspüren und zu umgehen => Weiterentwicklung von Sebek

Georgia Institute of Technology

- Aufbau:
  - Ähnlich, wie an der RWTH Aachen
  - 8 Honeypots
- Ergebnisse:
  - Viele – auch erfolgreiche - Angriffe auf das System entdeckt
  - Entdeckung einer kompromittierten Maschine im Universitätsnetz, die das Rechenzentrum auch nach Hinweis nicht finden konnte
  - Inzwischen: Einsatz des Honeynets als Sicherheitswerkzeug für die Universität

Inhalt

Zusammenfassung

- Mächtiges Werkzeug für die Forschung
- Neue Ansätze für Netzwerksicherheit
- Einfache technische Umsetzung
- Wichtig bei der Umsetzung:
  - Schutz des restlichen Netzes
  - Verantwortung für Angriffe aus dem Honeynet

ENDE