



Ermittlung von Verwundbarkeiten mit elektronischen Ködern

Maximillian Dornseif, Felix C. Gärtner, **Thorsten Holz**
(Lehr- und Forschungsgebiet Informatik 4)





Elektronische Köder – Honeypots

„Angenommen“, sagte er [Winnie Pu] zu Ferkel, „*du* willst *mich* fangen, wie würdest Du das machen?“

„Tja“, sagte Ferkel, „ich würde es so machen: Ich würde eine Falle bauen, und ich würde einen Topf Honig in die Falle stellen, und Du würdest den Honig riechen, und Du würdest in die Falle gehen, und ...“

Milne, A. *Pu der Bär*, 1987





- Sinn und Zweck von *honeynets*
- Aufbau des *honeynets* an der RWTH Aachen
- Bisherige Ergebnisse
- Ethische und rechtliche Aspekte
- Weitere Arbeiten



- Netzwerkressource (Computer, Router, Switch, . . .), die getestet, angegriffen und kompromittiert werden soll
- Keine Aufgabe im Netz, möglichst nicht unterscheidbar von regulären Ressourcen
- Modifikation des *honeypot*, um forensische Untersuchungen zu vereinfachen



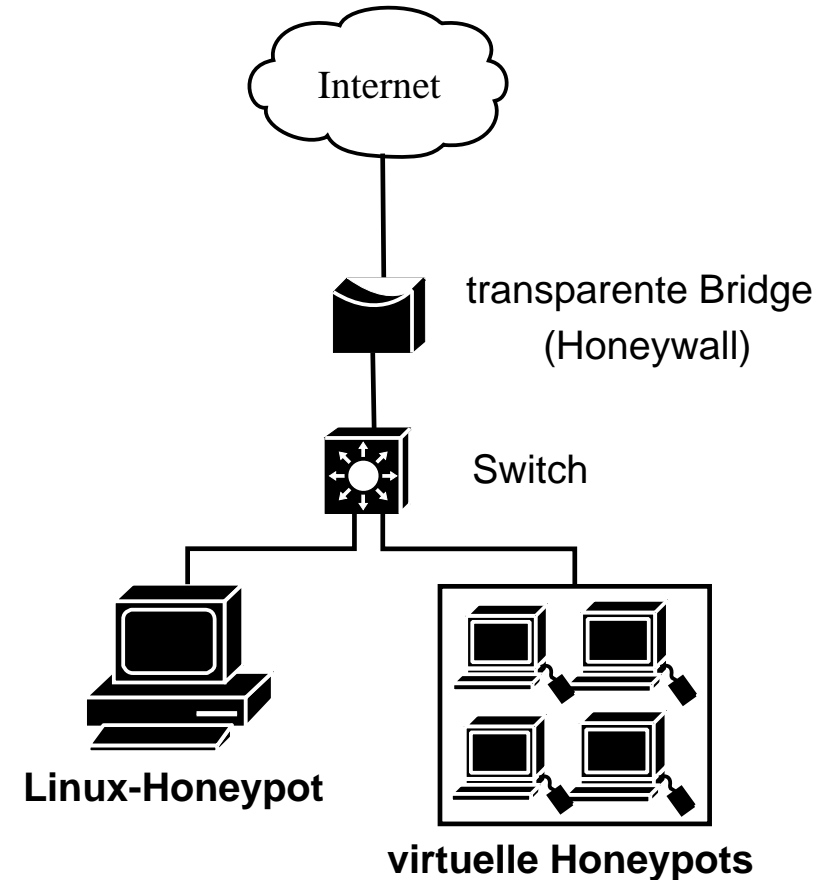
- Internationaler Zusammenschluss von Forschern aus der IT-Sicherheit
- Ziele des Projekts
 - Bewusstsein schaffen
 - Lernen über bekannte Angriffswege
 - Lernen über unbekannte Angriffswege
 - Aktive Verteidigung



- Entwicklung von Werkzeugen, beispielsweise Überwachungssoftware *Sebek* oder Software zur Datenanalyse
- Bisherige Erfahrungen mit *honeynets*
 - Vorgehensweise und verwendete Tools von Angreifern
 - Informationen über soziales Verhalten durch Mitschnitte im *IRC*
 - Informationen über sogenannte *Botnets*

Weitere Informationen: <http://www.honeynet.org/>

- Transparente Bridge: Steuerung des Datenflusses und Aufzeichnung der Daten
 - *IDS* snort, *IPS* snort_inline
 - netfilter/iptables
- Linux-Honeypot mit SuSE Linux 7.2
- Mehrere virtuelle Rechner (Windows, FreeBSD, Linux)
- Angebotene Dienste: HTTP, FTP, SSH, ...





- Bisher keine Kompromittierung
- Interessante quantitative Ergebnisse (Linux-Honeypot bis April 2004)
 - Mehr als 425.000 Pakete
 - Mehr als 9.500 verschiedene IP-Adressen, vermutlich viele gefälscht
 - Mehr als 97% des Verkehrs ist TCP, jeweils 1.5% ICMP und UDP
 - Portscans vor allem nach ports 445/13* oder 80
 - Fast 10.000 scans nach Hintertüren (`cmd.exe/root.exe`)
 - Keine fortgeschrittenen Techniken (SQL Injection o. ä.)



Auswertung der Honeyds – Juni 2004

Top 5 Accessed Ressources

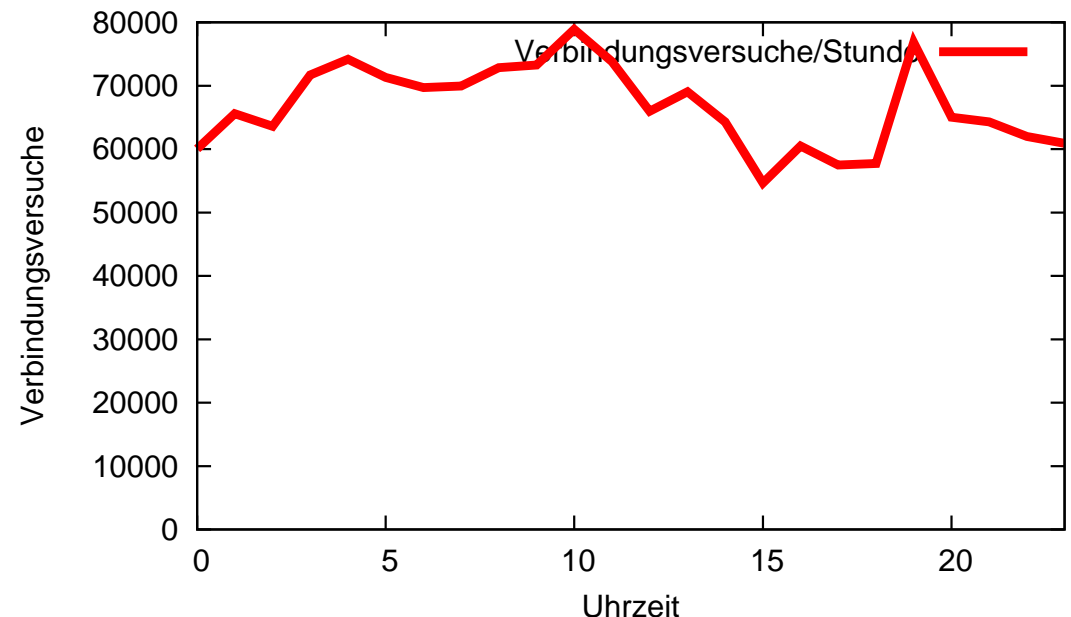
445/tcp	--	678489
139/tcp	--	339172
137/udp	--	190217
135/tcp	--	105395
80/tcp	--	44055

Top 5 Source Hosts

68.213.109.221	--	56703
206.51.65.29	--	52449
63.194.19.76	--	37996
4.22.154.47	--	29997
80.24.124.180	--	27848

Anzahl Verbindungen

Total:	1603559
TCP:	1343328
UDP:	205289
ICMP:	54942





- Zwei Fragen sind diskussionswürdig
 - Wie ist das *honeynet* in Bezug auf das gesamte Internet und wie sind insbesondere Angriffe von *honeypots* aus auf andere Systeme zu beurteilen? (ethische, straf- und zivilrechtliche Aspekte)
 - Wie ist es zu bewerten, dass die Angreifer ohne ihr Wissen zum Teil eines Experimentes gemacht werden? (Datenschutz)



Straf- oder zivilrechtliche Haftung bei Angriff gegen Dritte?

- Strafrechtliche Aspekte

- § 27 StGB („Beihilfe“) nicht anwendbar, da keine vorsätzliche Hilfeleistung erfolgt (`snort_inline`, `iptables...`)
- Betrieb eines Rechners mit dem Sicherheitsniveau der *honeypots* völlig sozialadäquat

⇒ Strafrechtlich ist der Betrieb eines *honeynet* unbedenklich.



- Zivilrechtliche Aspekte
 - § 823 I BGB („Schadensersatzpflicht“): Zurechenbarkeit des durch Angreifer verursachten Schadens?
 - Haftung aus dem Unterlassen der Absicherung des *honeynets* (Verkehrssicherungspflicht)?
 - Gesellschaft inklusive Rechtsprechung lehnen Schadensersatzpflicht für Schäden durch unsichere Systeme bisher ab
- ⇒ Verkehrssicherungspflicht erfüllt, also niedriges Risiko für zivilrechtliche Klagen



- Datenschutzrechtliche Aspekte
 - Kein Kontakt mit personenbezogenen Daten
 - Wissen über *honeynets* verbreitet; Angreifer nehmen Aufzeichnung und Untersuchung ihres Handelns billigend in Kauf

⇒ Keine datenschutzrechtlichen Bedenken
- Ethische Aspekte
 - Ergebnisse tragen mittelfristig zur Steigerung der Gesamtsicherheit des Internet bei
 - Durch Absicherung des *honeynets* keine höhere Gefahr für Dritte



- Verteilte *honeynets* auf Basis von `honeyd`
Gemeinsame Arbeit mit dem *French Honeynet Project*
- Gründung des *German Honeynet Project*
- Veröffentlichungen:
 - Dornseif, Holz, Klein: „NoSEBrEaK – Attacking Honeynets“
(Best Paper Award bei 5th IEEE IAW, Westpoint)
 - Dornseif, May: „Modelling the costs and benefits of Honeynets“
(WEIS04, Minneapolis)
 - Dornseif, Holz, Mathes, Weisemöller: „Measuring Security Threats with Honeynet Technology“ (SANE 2004, Amsterdam)



Vielen Dank für ihre Aufmerksamkeit!

Weitere Informationen:

<http://www-i4.informatik.rwth-aachen.de/lufg/honeynet>

Erreichbar unter:

{dornseif|gaertner|holz}@i4.informatik.rwth-aachen.de

RWTH RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

