

# Aufbau und Betrieb von Honeypot-Systemen

Lukas Grunwald

DN-Systems Enterprise Internet Solutions GmbH, Germany

**DNS**

DN-Systems  
Enterprise  
Internet  
Solutions  
G m b H

# Agenda

- Theorie
  - Aufgaben eines Honeypots
  - Definition Honeypot
  - Ausprägungen
  - Analyse

# Agenda

- Praktischer Aufbau von Systemen
  - Aufbau
  - Timekeeping
  - Test mit Werkzeugen von Angreifern
  - Überwachung
  - Auswertung

# Theorie

## Herkömmliche Sicherheitsinstrumente im Netz:

- IDS
- IPS
- VPN
- Firewalls
- Gateways

# Warum ein Honeypot ?

- als Instrument zur Verteidigung sensibler IT-Systeme
- HP-Systeme sollen die Eindringlinge von den wichtigen Systemen fernhalten
- Analyse von Angriffen
- Prävention

# Aufgaben eines Honeypots

- Überwachung von Daten oder Ereignissen (Monitoring)
- Filtern von Datenpaketen (Filtering)
- Einbruchsalarm (Intrusion Detection)
- Systemüberprüfung (Audit)
- Gegenmaßnahmen (Escalation)

# Umfeld im Unternehmen

Diese Aufgaben sind im Unternehmen organisatorisch in einen Prozess einzubinden, der gewährleistet, dass alle anfallenden Daten ausgewertet und den verantwortlichen Personen oder Instanzen zugeführt werden.

# Definition Honeypot

**Ein Honeypot ist ein fiktives, sicherheitstechnisch verwundbares System, das als Falle für nicht-legitimierte Benutzer und Angreifer fungieren soll.**

# Ausprägungen

Im Kommerziellen Umfeld (1/2):

- um sicherheitskritische Angriffe auf sich zu ziehen
- um die Ressourcen des Angreifers zu erschöpfen
- um Hinweise zu noch unbekanntem Angriffsszenarien zu erhalten
- um als Frühwarnsystem zu agieren.

# Ausprägungen

Im Kommerziellen Umfeld (2/2):

- um Beweismittel für den Vorsatz der Tat in juristisch verwertbarer Form zu dokumentieren
- um die strafrechtliche Identifikation des Angreifers zu ermöglichen
- um Konflikte mit geltendem Arbeitsrecht und Datenschutz zu vermeiden

# Ausprägungen

Im Umfeld der Forschung und Lehre:

- Erforschung der Ziele von Angreifern
- Analyse von neuen Angriffswerkzeugen
  - Strategien
  - Philosophien
- Erforschung neuer Angriffvarianten
- Typisierung von Angreifern
- Täter- und Persönlichkeitsanalysen

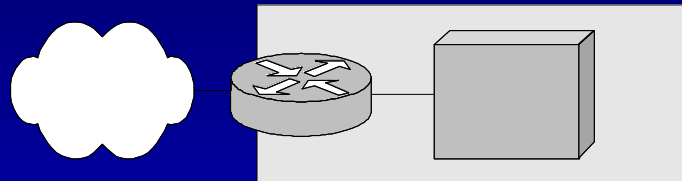
# Honeypot-Typen

Man unterscheidet hostbasierende Honeypot- und netzbasierende Honey-net-Varianten. Diese lassen sich nach derzeitigem Stand der Technik in folgende Untergruppen einteilen:

# Type 1

Eigenständiges System, welches via Sicherheits-Hardware angebunden ist (Vollinstallation: Speziell notwendig für eine forensische Analyse).

Beispiel: Ein Opferrechner auf der Basis alter i586-Hardware.

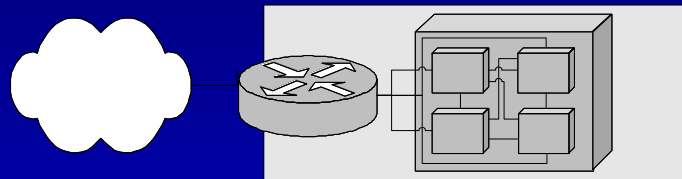


# Type 2

Logisch Eigenständiges System

Vollinstallation (virtuell; wirtschaftlich sinnvoll, um mehrere Systeme auf einer Hardware zu betreiben), etwa auf der Basis von Virtual Machines (VM).

Beispiel: Usermode Linux, welches als Honeygot einen Server laufen lässt.



# Type 3

Emulation; One-to-One-Beziehung

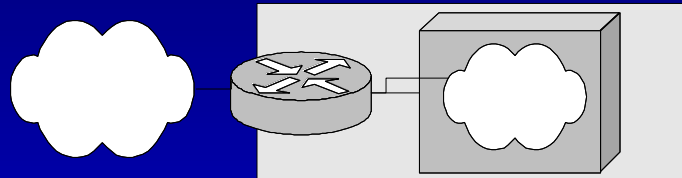
(einfache, realitätsnahe Darstellung), beispielsweise shadow, dtk

# Type 4

Emulation; One-to-Many-Beziehung

Hier wird, ohne reelle Hardware zu besitzen, eine komplexe, realitätsnahe Darstellung kompletter IT-Strukturen im Netzwerk mit konnektierten Hosts, Routern und Servern emuliert.

Beispiel: Virtuelles Netzwerk mit Honeyd

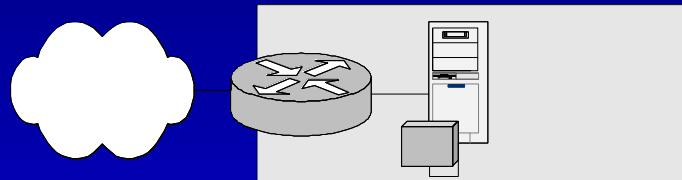


# Type 5

## Punktuelle Fallen (Traps)

Diese Fallen werden auf Produktiv-Servern an speziellen kritischen Schaltstellen - wie dem Mailserver - installiert. Sobald jemand in diese Falle tappt, wird eine Eskalation durchgeführt.

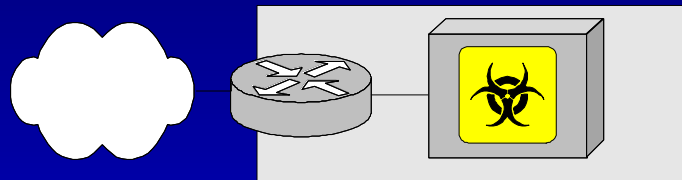
Beispiel: "netcat -p 23öder LaBrea, um Code Red und andere Würmer auszubremsen.



# Type 6

## Poisoned Honeypot

Die Typen 1-5 werden mit "Malicious Code" (Viren, Würmer, Trojaner) ausgestattet. Dadurch entsteht ein so genannter poisoned Honeypot (vergifteter Köder). Diese Variante ist manchmal im militärischen Umfeld möglich, da solch ein System aktiv zurückschlägt.



# Täter

Es gibt eine Vielzahl von Angreifern und suspekten Personen, die in ein Honeypot-System einzudringen versuchen.

Als Täter kommen verschiedene Persönlichkeiten in Betracht, welche unterschiedliche Bedrohungsszenarien darstellen.

# Skript-Kinder

- Motivation, andere Leute zu verärgern und Schaden anzurichten
- i.d.R. jugendliche Personen
- relativ niedriger Wissensstand
- benutzen meistens Tools und Werkzeuge von so genannten Hacker-Pages
- Massenphänomen
- ziel- und wahllose Angriffe auf Hosts
- verursachen den meisten relevanten Verkehr für Honeypots
- Angriffe basieren auf Port-Scannern und anderen Tools

# Hacker

- Motivation, anderen ihre Kenntnisse zu demonstrieren
- relativ hoher Wissensstand
- beschränkte finanzielle Ressourcen
- benutzen eigene Tools und Werkzeuge
- inzwischen eher selten
- arbeiten aber i.d.R. nicht kommerziell
- verursachen den für Honeypots relevanten Verkehr

# Cracker

- Cracker ist die kriminelle Version des Hackers
- bessere monetäre Ressourcen
- professioneller bzw. kommerzieller Hintergrund
- arbeitet im Bereich der Industriespionage
- sucht nach Industrie- und Regierungsgeheimnissen
- Hauptmotiv ist Geld
- ist als professioneller Krimineller einzustufen

# Werbemailversender

- neu auftretendes Phänomen
- suchen gezielt Rechner mit Schwachstellen, um SPAM zu versenden
- professioneller bzw. kommerzieller Hintergrund
- verärgerende Werbebotschaft auf Kosten Dritter
- Hauptmotiv ist Geld
- ist als Krimineller einzustufen

# Praktischer Aufbau

Seit 1999 wurde eine Vielzahl von kommerziellen und nicht-kommerziellen Produkten bzw. Paketen für die Honey-Techniken entwickelt.

Für die Erprobung in der Praxis und die Vorbereitungen im Unternehmen bietet sich zunächst das Testen mit freien Produkten an. Das spart überdies Lizenzkosten.

# Aufbau

Folgende Voraussetzungen sind notwendig:

- keine Firewall
- optional ein IDS/IPS
- Port-Monitor oder HD-Hub Layer-2 Ethernet
- Sniffer
- Zentrale Kontrollstelle

# Timekeeping

Damit die einzelnen Ereignisse korreliert werden können, ist es notwendig, für alle Komponenten des Systems, wie z.B. einen Typ-1 oder einen Typ-5-Honeypot, ein Timekeeping-System einzuführen.

In der Praxis hat sich ein NTP-System als sinnvoll erwiesen. Dabei ist darauf zu achten, dass die geringeren Stratum-Server unbedingt durch die vom NTP unterstützten ACLs gegen eine Manipulation vom Honeypot-System abgesichert werden.

# Timekeeping

```
# NTP configuration file for the NTP-Server
# Ignore all Requests

restrict default ignore

# Allow Administration via ntpq
restrict 127.0.0.1
#
# Network Clients
restrict 192.168.101.0 mask 255.255.255.0 nomodify # honey-net
restrict 192.53.103.103
restrict 192.53.103.104
server 192.53.103.103 #ntp1.ptb.de
server 192.53.103.104 #ntp2.ptb.de
fudge 127.127.1.0 stratum 10 # local clock is unsynchronized restrict
```

# DNS und Hostname

Bei dem Eintrag des Netzes bzw. der Host-Adresse in den DNS-Server sollte vermieden werden, dass ein Angreifer auf den "wahren Zweck dieses Systems schließen kann. In diesem Zusammenhang sollte auf die folgenden Punkte geachtet werden:

- Namen wie A-Records oder MX-Einträge wie honey.myzone.de sind zu vermeiden
- der Hostname darf nicht via SMTP Banner den Zweck des Rechners verraten

# DNS und Hostname

Aber auch wenn das System sich unter "honeypot.myzone.com" meldet, hält es die Masse der Angreifer nicht davon ab, ihre Kenntnisse zu demonstrieren und uns den notwendigen Hintergrund zu liefern.

# Süße Versuchung

Oft ist es sinnvoll, einem scheinbar lohnenden Ziel weitere Anreize zu bieten. Gerade im Firmenumfeld können absichtlich platzierte falsche Dokumente auf einem Honeypot-System helfen, einen Innentäter zu ertappen und ihn auf diese Weise zu überführen.

# Tests mit Hackertools

Nachdem ein System installiert worden ist, muss kontrolliert werden, ob es seinen Zweck erfüllt. Dazu kann mit Angriffstools verifiziert werden, ob:

- Informationen übermittelt werden, welche auf den eigentlichen Zweck des Systems schließen lassen,
- der angebotene Port auch tatsächlich vorhanden ist,
- Alarmierungssysteme, Kontroll- und Beobachtungseinrichtungen funktionieren
- das System gegen die übrigen Produktionssysteme abgeschottet ist.

# Überwachung

Wir überwachen:

- gesamte Kommunikation
- jegliches außergewöhnliche Verhalten
- bei VM-Installationen alle Änderungen in der VM

Dadurch hat man jederzeit die Möglichkeit, den aktuellen Stand des Systems einzufrieren, zu analysieren und die Kommunikation über die Systemgrenzen zu kontrollieren.

# Notbremse

Einen äußerst wichtigen Stellenwert beim Betrieb eines Honeypot-Systems nimmt die Notbremse ein. Diese kann z.B. über ein einfaches Perl-Skript erfolgen, welches eine IP-Rule etabliert. Sobald der Verkehr auf dem Honeypot-System schlagartig ansteigt oder versucht wird, andere Rechner in der DMZ von Honeypot-Systemen anzugreifen, wird die Notbremse aktiv.

- Durch eine Not-Aus-Funktion wie eine Firewall-Regel ist gewährleistet, dass bei einem Übernahmeversuch der Angriff weitestgehend auf die Honeypot-Zone beschränkt bleibt.

# Auswertung Rechnerinhalt

Diese Auswertung kann nur von einem sogenannten Analyse-System, welches nicht im Honeypot-Umfeld lokalisiert ist, durchgeführt werden. Nachdem das ursprüngliche File-System - sofern es noch verfügbar ist - read-only gemountet worden ist, wird zunächst eine Integritätsüberprüfung der System-Binaries durchgeführt.

# Auswertung Logfiles

Neben dem Auswerten der Daten des Honeypot-Systems empfiehlt es sich, auch die Logfiles auszuwerten, die z.B. auf einem anderen Kanal auf dem Host-System im uptime-Modus gesichert wurden. Diese Logfiles geben Aufschluss über Kommunikationsbeziehungen der Systeme untereinander sowie versuchte Angriffe.

# Netzwerkverkehr

Damit der Netzwerkverkehr ausgewertet werden kann, ist es sinnvoll, diesen im PCAP-Format zu speichern. Eine Analyse kann mit freien Tools wie EtherReal oder TCPDUMP durchgeführt werden. Verdächtige Stellen im Datenstrom des Netzwerkverkehrs werden festgestellt durch:

- Einträge im Syslog,
- Meldungen von der Firewall,
- Verkehrsänderungen,
- durch das GIDS,
- durch markiertes Verhalten.

# TCPDUMP

Nachdem diese Stellen gefunden sind, kann nun eine Analyse der Pakete z.B. mit TCPDUMP erfolgen.

```
02:38:41.523741 67.75.67.147.5625 > 193.108.181.24.8080: S 674719801
03:21:43.720708 67.75.67.147.5625 > 193.108.181.42.8080: S 674719801
03:39:30.089344 216.218.158.87.1057 > 193.108.181.8.1434: udp 376
04:16:08.657626 62.135.27.130.1652 > 193.108.181.8.1434: udp 376
04:24:02.581537 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
04:24:06.503391 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
04:24:10.571422 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
04:25:01.337934 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
04:25:09.368497 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
05:20:17.966979 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
05:20:26.006505 209.67.2.126 > 193.108.181.6: icmp: host 165.251.41.
05:37:17.807893 200.203.120.200.3206 > 193.108.181.6.1434: udp 376
05:53:27.096218 68.32.17.41.4302 > 193.108.181.42.1434: udp 376
06:54:20.742452 68.226.158.136.2789 > 193.108.181.6.80: P 3880322941
ack 4276001828 win 64240 (DF)
07:02:42.270314 216.218.158.87.1057 > 193.108.181.42.1434: udp 376
07:05:53.159239 66.196.90.216.44526 > 193.108.181.6.80: P 3278756138
ack 680530510 win 5840 (seq 20282 timestamp 20282)
```

**DNS**

DN-Systems  
Enterprise  
Internet  
Solutions  
G m b H

# SMTP - Honeypot

Aufgabe eines SMTP Honeypot ist es, Versuche von Spammern zu erkennen, ihre Werbemails zu relayen bzw. eine Mail über dieses System auszuliefern.

Die Quelle der IP-Adressen von den Spam-Sendern werden in eine DNS-Zone eingetragen, so dass diese Systeme über eine Realtime-Blockingliste von den eigentlichen Produktiv-MTAs blockiert werden können.

Durch ein gezieltes Platzieren der SMTP-Sensoren ist es möglich, neue SPAM-Sender schnell zu erkennen und auszuschalten.

# Systemaufbau

Direkt an das Internet angeschlossen ist ein Debian GNU/Linux-System, auf dem der Exim 3.0 MTA als Pseudo-MTA fungiert.

Dabei ist die MTA-Konfiguration wie folgt zu ändern:

# Systemaufbau

Durch diese Option akzeptiert der MTA jeden Relayversuch zu einer gültigen EMail-Adresse. Nicht-konnectierte Zonen werden dennoch abgewiesen.

```
# The setting below allows your host to be used as a mail relay only by  
# localhost: it locks out the use of your host as a mail relay by any  
# other host. See the section of the manual entitled "Control of relaying"  
# for more info.
```

```
host_accept_relay = *
```

# Neuer Transport

Dann muss bei den Transports ein neuer Transport installiert werden, der dann den Remote-SMTP ersetzen kann.

```
#####  
#          TRANSPORTS CONFIGURATION          #  
#####  
  
forensic_delivery:  
driver = appendfile  
directory = /var/spool/hsmtplib/mail  
delivery_date_add  
maildir_format  
envelope_to_add  
return_path_add  
user = mail  
group = mail  
mode = 0660
```

# Router

Nun muss der Mail-Router von `remote_smtp` auf den neuen `forensic_delivery` Transport umgestellt werden.

```
lookuphost:
```

```
    driver = lookuphost
```

```
transport = forensic_delivery
```

```
literal:
```

```
    driver = ipliteral
```

```
transport = forensic_delivery
```

```
end
```

# Live-System

Schon nach wenigen Minuten werden die ersten Systeme versuchen, ihre Werbebotschaften über den Open-Relay zu verteilen. Im Exim-Logfile ist dann so etwas oder ähnliches zu lesen:

```
2004-02-25 14:39:55 1AvzGU-0001jG-00 <= session12002@yahoo.com
H=slip-12-65-114-33.mis.prserv.net (mx2.mail.yahoo.com) [12.65.114.33 ]
P=esmtpl S=831
id=049057051046049048056046049056049046049048050@mx2.mail.yahoo.com
2004-02-25 14:39:55 1AvzGU-0001jG-00 => smtps1@cox.net R=lookuphost
T=forensic_delivery H=mx.east.cox.net
2004-02-25 14:39:55 1AvzGU-0001jG-00 Completed
[...]
```

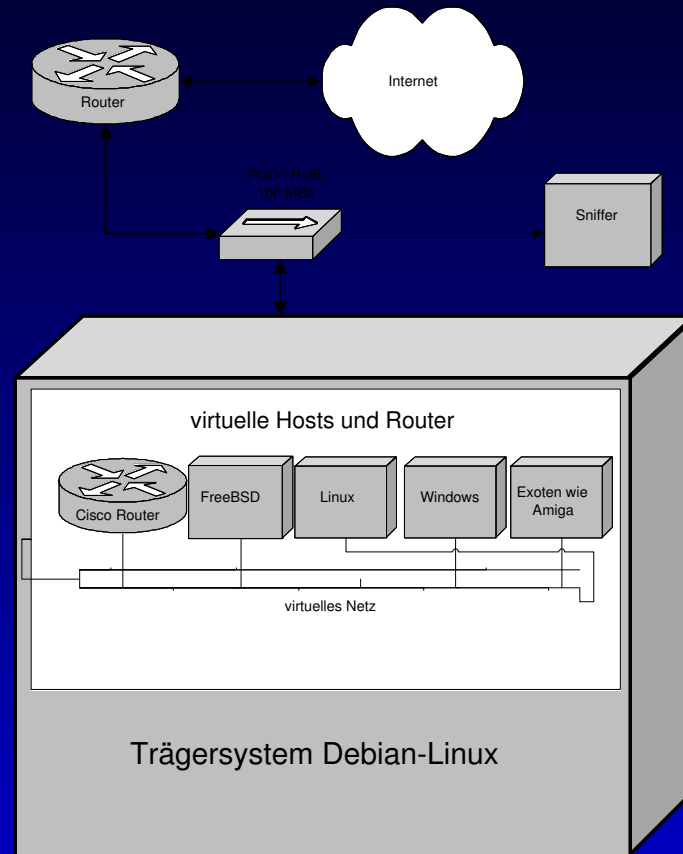
# Wireless Technologie

Im Gegensatz zu den drahtgebundenen Techniken stellt die Wireless-Technologie eine weitere Herausforderung für den Betrieb von Honeypot-Systemen dar. Über einen weiteren physikalischen Layer, den so genannten Connection-Layer, können sich andere Beteiligte in der Reichweite des Umfeldes in das Netz miteinspeisen, ohne dass sie physikalischen Zugang zu irgendwelchen Kommunikationsleitungen oder dem Betriebsgelände haben. Zu diesem Thema erfolgt eine praktische Demonstration !

# Honeyd - Ein Honeynet

Eine weitere Möglichkeit zum Absichern von wireless und drahtgebundenen Netzen besteht mit so genannten Honeynetzen. Im Gegensatz zu einem Honeytrap wird bei einem Honeynet die gesamte Infrastruktur simuliert inklusive Schwachstellen, wobei auch bei dieser Simulation Auswertungsskripte bzw. Aktionen - wie z.B. das Sperren von Firewall Ports oder das Alarmieren - ausgeführt werden können.

# Aufbau



# Literatur

- [1] Süße Falle, Honey-Techniken zur Einbruchsvorsorge – Lukas Grunwald, Jochen Schlichting <http://www.heise.de/ix>, (2003).
- [2] Honeyd - Network Rhapsody for You <http://www.citi.umich.edu/u/provos/h> (2004).
- [3] Running a wireless Honeypot on CeBIT 2003 <http://www.phreak.de/cebit2003>, (2003).