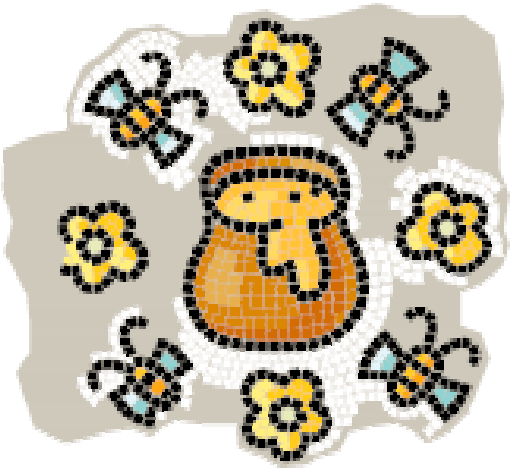
Honeypots



Wei Wei
Xu Zhiyao

FH, Gelsenkirchen, Informatik, Netzwerksicherheit
Dozent: Prof. Dr. Norbert Pohlmann
12.01.04

Inhalt des Vortrags

- **Übersicht**
  - Geschichte, Definition, Ziele, Vorteile und Nachteile, Klassifikation
- **Beispiele**
  - BackOffice Friendly, Honeynet, usw.

Geschichte

- **Frühe Publikationen:**
  - **1990/1991—** First public works documenting honeypot concepts—Clifford Stoll's *The Cuckoo's Egg* und Bill Cheswick's *An Evening With Berferd.*
- **Frühe Produkte:**
  - **1997—** Version 0.1 of Fred Cohen's Deception Toolkit was released, one of the first honeypot solutions available to the security community.
- **Honeypots in Aktion:**
  - **2000/2001—** Use of honeypots to capture and study worm activity. More organizations adopting honeypots for both detecting attacks and for researching new threats.

Definition

- Was ist ein Honeypot?
  - **A honeypot is security resource whose value lies in being probed, attacked, or compromised.**

—— Lance Spitzner

(Eine Sicherheits-Resource, deren Wert darin liegt, ausspioniert, attakiert, bzw. kompromittiert zu werden)

- Forderungen:
  - **Es werden keine Produktionsdienste angeboten**
  - **Es gibt keine autorisierte Nutzung**
  - **Verbindungsaufbau zum Honeypot ist im Allgemeinen ein Scan oder ein Angriff**
  - **Verbindungsaufbau vom Honeypot bedeutet das System wurde kompromittiert**

Wie funktioniert ein Honeypot?

- Bewachen einige Ports
- Emulation von Diensten

  u.U. mit bekannten Verwundbarkeiten
- Loggen alle versuchte Angriff
- usw.

  (wird später in Beispiele gezeigt.)

Ziele des Honeypots

- **Ziel des Ganzen ist es entweder, seine "echten" Netze zu schützen, oder man möchte etwas über die Motivation, Techniken und Werkzeuge der Angreifer lernen**
  - Honeypots ist ein vorgeschaltete „Fake“ Netz, wo einege „Loch“ enthalt. Es kann die Aufmerksamkeit der Hackern von „echten“ Netze ablenken
  - Know your enemy

    jede Schritt eines Angreifers wird in ein Logbuch gespeichert
  - Erkennen von neuen Angriffen

    wenn Honeypots in eine Interval mehre mal gescannt wird, dann gibt es eine Möglichkeit des neues Angriffs
  - Entwickeln von Gegenmassnahmen

    wenn man seine Feinde kennt, kann er selbe Technologie verbessern.

Vorteile (1/2)

- **Einfachheit des Konzepts**
  - Im Gegensatz zu anderen Sicherheitsmechanismen, wie z.B. Firewalls oder IDS, sind beim Einsatz von Honeypots keine Filterregeln oder Signaturen notwendig, deren Güte die Wirksamkeit der Maßnahme unmittelbar bestimmt.
- **Die gesammelten Daten haben einen hohen Informationswert**
  - Da es keine autorisierte Nutzung von Honeypots gibt und Verbindungen daher im Allgemeinen einen Angriff darstellen, haben die mit einem Honeypot gesammelten Daten einen hohen Informationswert bzgl. Sicherheitsvorfällen. Dadurch treten auf der einen Seite wenige ”False Positives“ auf (Alarmierung, obwohl kein Angriff erfolgt). Auf der anderen Seite ist es durch das relativ geringe Datenaufkommen möglich, alle entstehenden Daten zu sammeln bzw. bei jedem Verbindungsaufbau zu alarmieren. Dadurch gibt es wenige False Negatives (keine Alarmierung, obwohl ein Angriff erfolgt).

Vorteile (2/2)

- **Betrieb ist relativ wenig ressourcenintensiv**
  - Beim Einsatz von Honeypots müssen keine im Rahmen der Geschäftsprozesse anfallenden Daten verarbeitet werden. Daher ist auch beim Einsatz von wenig leistungsfähigen Systemen keine Überlastung durch zu hohes Datenaufkommen zu erwarten.
- **Die Gewinns von Investment**
  - Bei vielen, insbesondere vorbeugenden Maßnahmen ist es schwierig zu erkennen, welchen Wert diese haben. Beim Einsatz von Honeypots kann unmittelbar festgestellt werden, wie viele Angriffe erfolgreich waren bzw. gewesen wären und u.U. auch welches Ziel mit ihnen verfolgt wurde.

Nachteile

- **Eingeschränkte Sicht**
  - Findet ein Angriff statt und erfolgt dabei kein Zugriff auf den Honeypot, so besteht keine Möglichkeit, diesen Angriff mithilfe des Honeypots festzustellen
- **Es werden keine verwundbaren Systeme geschützt**
  - Durch den Einsatz von Honeypots wird keinen Verwundbarkeiten entgegengewirkt
- **Risiko**
  - Zunächst muss beachtet werden, dass auch Honeypots grundsätzlich von Angreifern kompromittiert werden und dann zur Durchführung weiterer Angriffe auf Dritte oder andere Systeme des eigenen Rechnernetzes genutzt werden können. Ferner besteht beim Einsatz von Honeypots grundsätzlich das Risiko, dass diese von Angreifern z.B. durch Fingerprinting als solche erkannt werden können

Klassifikation (1/2)

- **Nach die Rolle der Honeypots im allgemeinen Sicherheit**
  - Produktivitäts-Honeypots
    - Vorbeugung vor Angriffen (prevention)

      Zur Täuschung bzw. Abschreckung von Angreifern, nur eingeschränkt wirksam.
    - Erkennung von Angriffen (detection)

      Jeder Verbindungsaufbau stellt im Allgemeinen einen Angriff dar.
    - Reaktionen auf Angriffe (response)

      Untersuchung der Vorfalls wird nicht durch Produktionsabläufe behindert.
  - Forschungs-Honeypots
    - Sammeln von Informationen über Angreifer.
    - Frühwarnsystem für neue Exploits oder Würmer.
    - Most security measures are about keeping blackhats out. This one is different: It is about keeping the bad guys in.

Klassifikation (2/2)

- Nach Interaktionsmöglichkeiten
  - System mit hohen Interaktionsmöglichkeiten

    z.B. **BackOfficer Friendly , Specter , Honeyd**
  - System mit mittele Interaktionsmöglichkeiten

    z.B. **Homemade Honeypots , Man Trap**
  - System mit wenig Interaktionsmöglichkeiten

    z.B. **Honeynets**

Grad der Interaktion

- **Interaktionsmöglichkeiten für Angreifer**
  - Je höher die Interaktion desto mehr kann über Angriffe bzw. Angreifer gelernt werden
  - Je höher die Interaktion desto höher die Risiken
  - Je höher die Interaktion desto höher der Aufwand
  - Produktivitäts-Honeypots bieten eher niedrige Interaktionsmöglichkeiten
  - Forschungs-Honeypots bieten eher hohe Interaktionsmöglichkeiten

Niedrige Interaktion

- Sehr einfache Struktur, einfach zu installieren.
- Wenige Risikomöglichkeiten.
- Ihre Funktionen sind auch beschränkt

BOF(**BackOfficer Friendly**)

- BOF ist ein low-interaction production honeypot.
- BOF kann einfache FTP, telnet, SMTP, HTTP, oder BackOrifice Dienste simulieren.
- Ungleich anderer Honeypots ist BOF ursprünglich nicht als Honeypot benutzt worden, sondern war ein Werkzeug gegen

  den Trojaner Back Orifice.

Wie funktioniert BOF

- Es protokolliert alle Versuche sich mit dem System zu verbinden
- kann gefälschte Antworten zurücksenden, so dass der Hacker das Gefühl hat tatsächlich mit einem System verbunden zu sein.

Specter

- Nachteil von BOF
- Specter bietet mehrere Funktionen als BOF
- Es emuliert 13 verschiedene Operationssysteme.
- Hoher Emulationsgrad

Mittlere Interaktion

- Homemade Honeypots
- Man Trap
- Unterschied zwischen niedriger Interaktion und mittlerer Interaktion.
  - Mittlere Interaktion kann man selbst definieren und konfigurieren.
  - Kein emuliertes System
  - Hohe Eroberungskapazität.

Beispiel

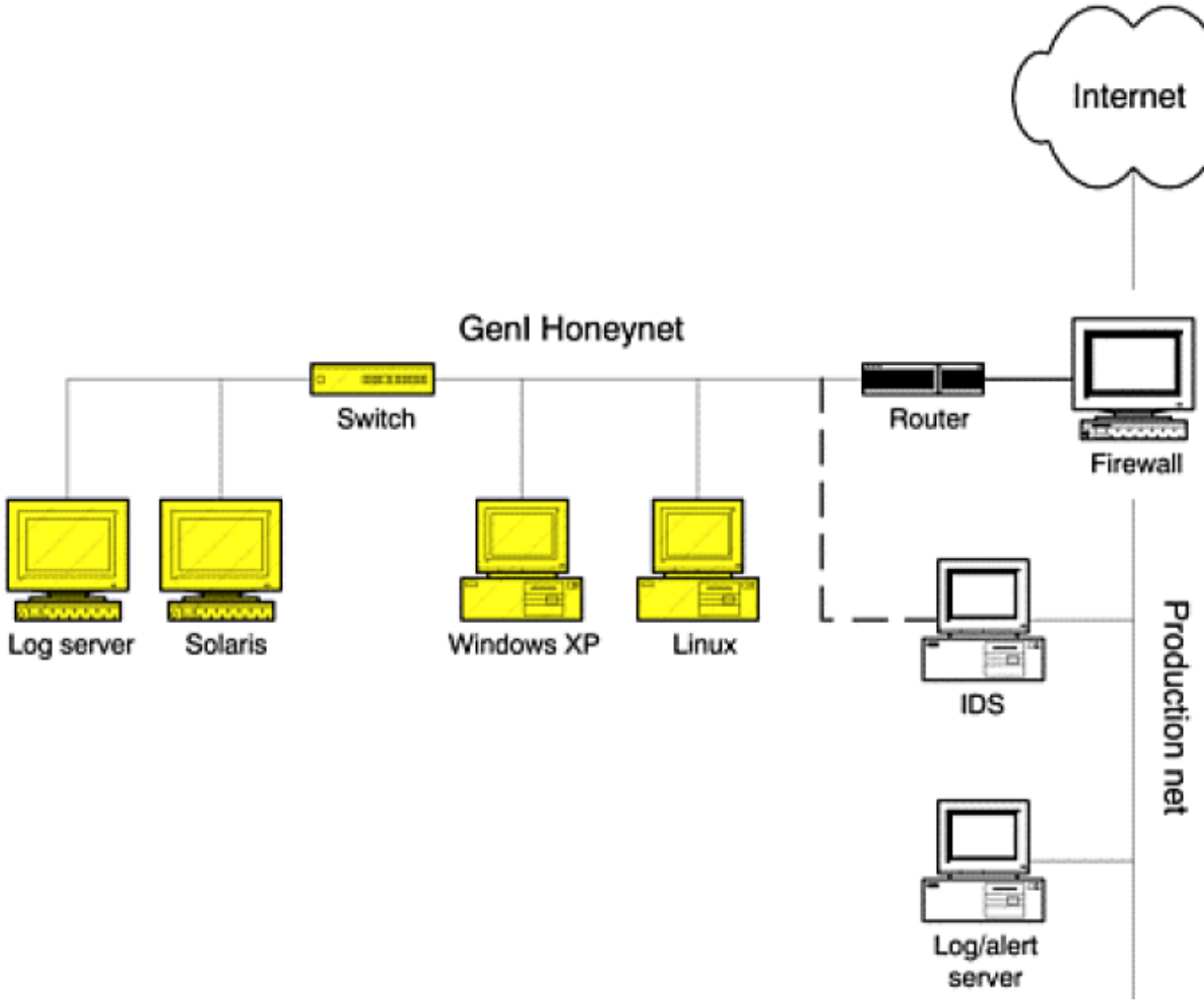
- Dieses Beispiel zeigt: wie registriert man das ganz Verhalten von Hackern. Ein Unterteil in Honeypot.
- Benötigte Software:
  - 1. ComLog
  - 2. wfpsetup
  - 3. ActivePerl-5.8.0.805-MSWin32-x86

Log File

Honeynet

- Das Konzept und die Entwicklung von Honeynet
  - Honeynet ist weder eine Software noch ein echtes System
  - Sondern eine Architektur.
- Hauptfunktionen
  - Datensammlung
  - Datenkontrolle
  - Datenregistrierung
- Architektur des Honeynets

Struktur von Honeynet



Literatur

- Addison Wesley: Honeypots - Tracking Hackers – 2002 -Lance Spitzner
- www.honeynet.org

Vielen Dank für Ihre Aufmerksamkeit