

Honeypots dan Honeynets

Mengapa HoneyPots

Banyak solusi keamanan di dunia TI bergantung pada honeypots. Honeypots memiliki kemampuan:

- Mampu membuat anti-virus signatures.
- Mampu membuat SPAM signatures dan filters.
- Mampu mengidentifikasi sistem yang disusupi.
- Mampu melacak jejak hacking.
- Dapat mencari dan menghapus botnets.
- Dapat menggumpulkan data dan menganalisis Malware.

Apa honeypot itu?

- Honeypots suatu vulnerable systems baik yang real atau virtual yang dipergunakan untuk memancing serangan.
- Kemampuan utama honeypots adalah dapat mengumpulkan informasi.
- Informasi ini digunakan untuk mengidentifikasi, memahami, dan melindungi terhadap ancaman dengan lebih baik.
- Honeypots melindungi jaringan.

Tujuan Honyepot

- ▶ Tujuannya adalah untuk meneliti dan menganalisis berbagai serangan
- ▶ Menciptakan anti virus signature.
- ▶ Membuat mekanisme filter SPAM berdasarkan signature email.
- ▶ ISP mengidentifikasi sistem yang disusupi.
- ▶ Membantu penegak hukum untuk melacak penjahat.
- ▶ Berburu dan mematikan botnet.
- ▶ Pengumpulan dan analisis malware.

Tipe-tipe Honeypot

Berdasarkan pemasangannya honeypot terdiri dari:

- Server: Letakkan honeypot di Internet dan biarkan orang jahat menyerang server honeypot.
- Klien: Honeypot memulai dan berinteraksi dengan server
- Lainnya: Proxy

Tipe-tipe Honeypot

► Low-interaction

- Tiru layanan, aplikasi, dan OS.
- Risiko rendah dan mudah diterapkan / dipelihara, tetapi dapatkan informasi terbatas.

► High-interaction

- Real service, aplikasi, dan OS
- Capture informasi yang luas, tetapi risiko tinggi dan waktu intensif untuk mempertahankan.

Tipe-tipe Honeypot

Production

- Mudah digunakan
- Capture informasi terbatas
- Terutama digunakan oleh perusahaan
- Ditempatkan di dalam jaringan produksi atau dengan server lain
- Biasanya interaksi rendah

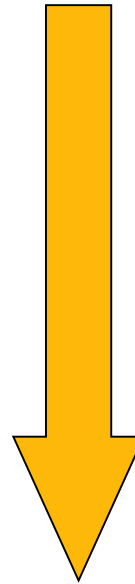
Research

- Susah untuk dibuat
- Capture informasi yang luas
- Terutama digunakan untuk penelitian, militer, atau pemerintah.

Contoh-contoh Honeypot

Low Interaction

- BackOfficer Friendly
- KFSensor
- Honeyd
- Honeynets



High Interaction

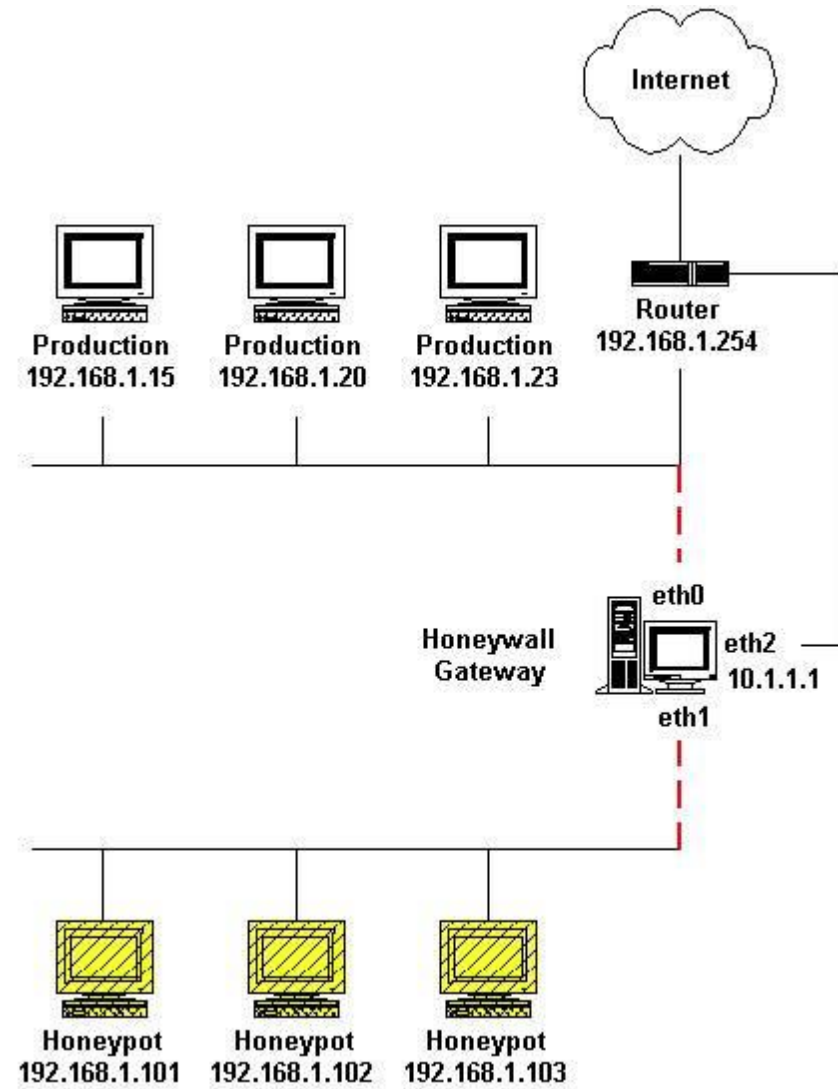
Honeynet

- High-interaction Honeypot dirancang untuk menangkap informasi mendalam.
- Ini adalah arsitektur yang sama dengan sistem asli, bukan berbentuk hardware atau software.
- Setiap lalu lintas yang masuk atau berangkat akan diawasi.

Bagaimana Honeynet bekerja

- Jaringan yang sangat terkontrol di mana setiap paket masuk atau keluar dipantau, ditangkap, dan dianalisis.
 - ✓ Kontrol Data
 - ✓ Pengambilan Data
 - ✓ Analisis data

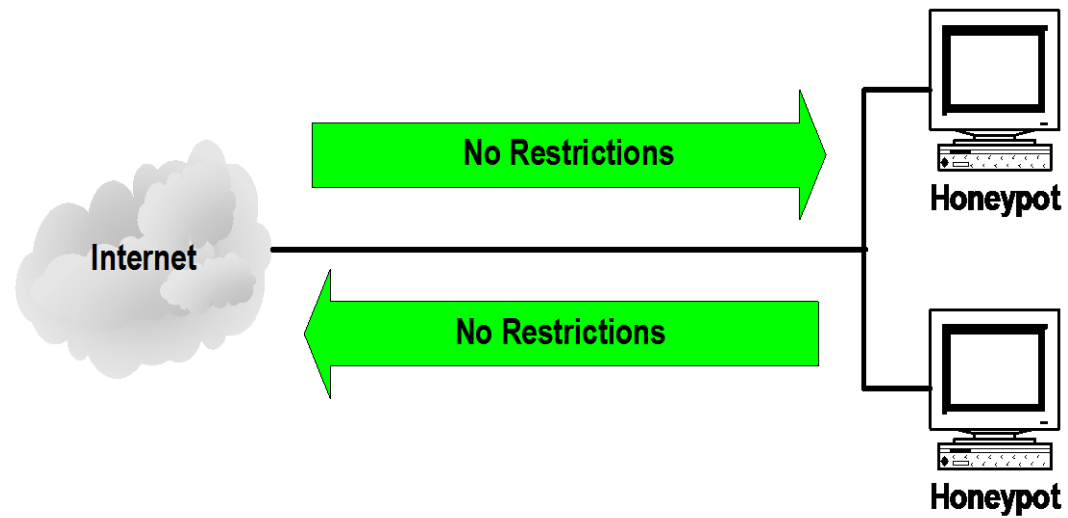
Arsitektur Honeynet



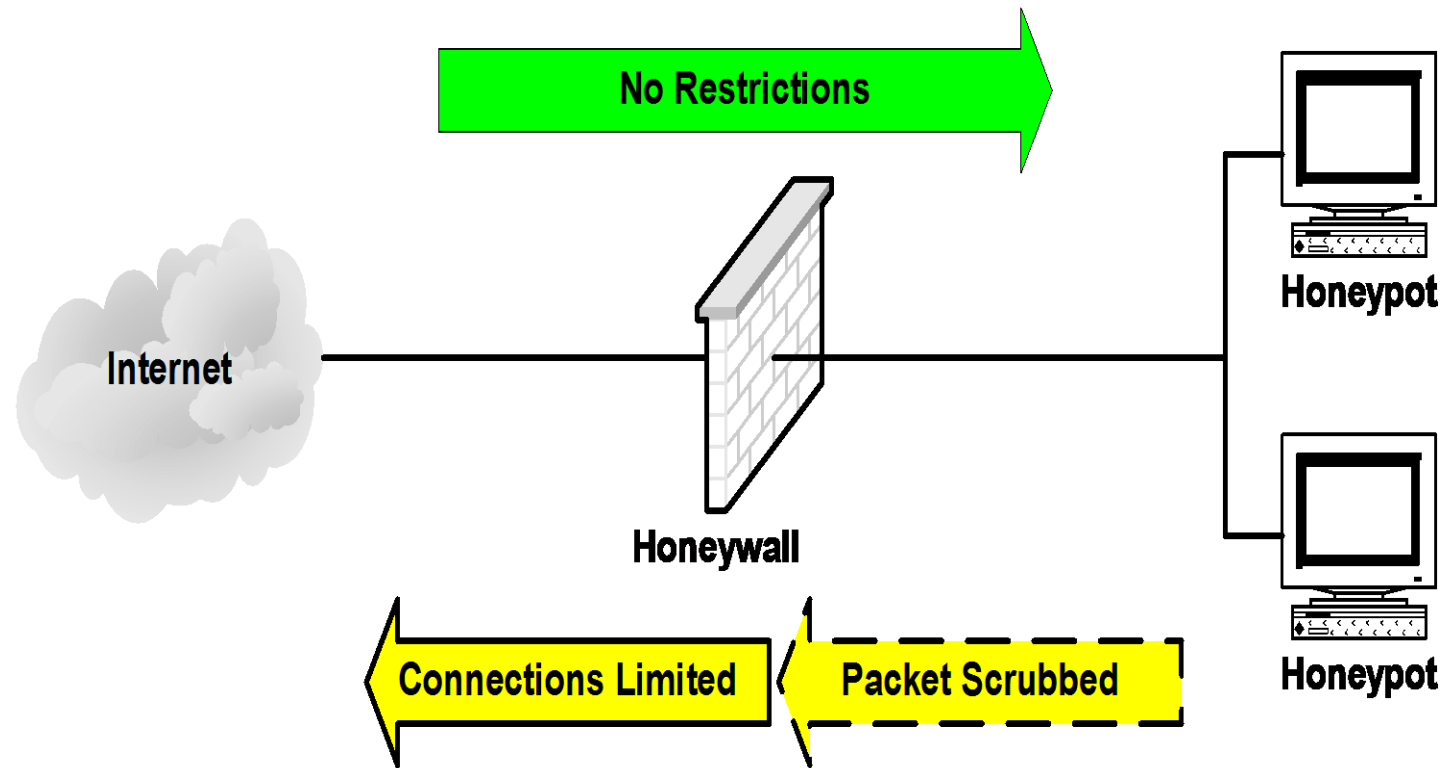
Kontrol Data

- Memitigasi risiko honeynet yang digunakan yang dapat merusak sistem sebenarnya.
- Memantau koneksi yang keluar.
- IPS (Snort-Inline)
- Membatasi penggunaan Bandwidth

Tanpa kontrol data



Dengan kontrol data



Pengambilan Data

- Catat semua aktivitas pada berbagai level.
 - ✓ Aktivitas jaringan.
 - ✓ Aktivitas aplikasi.
 - ✓ Aktivitas sistem.

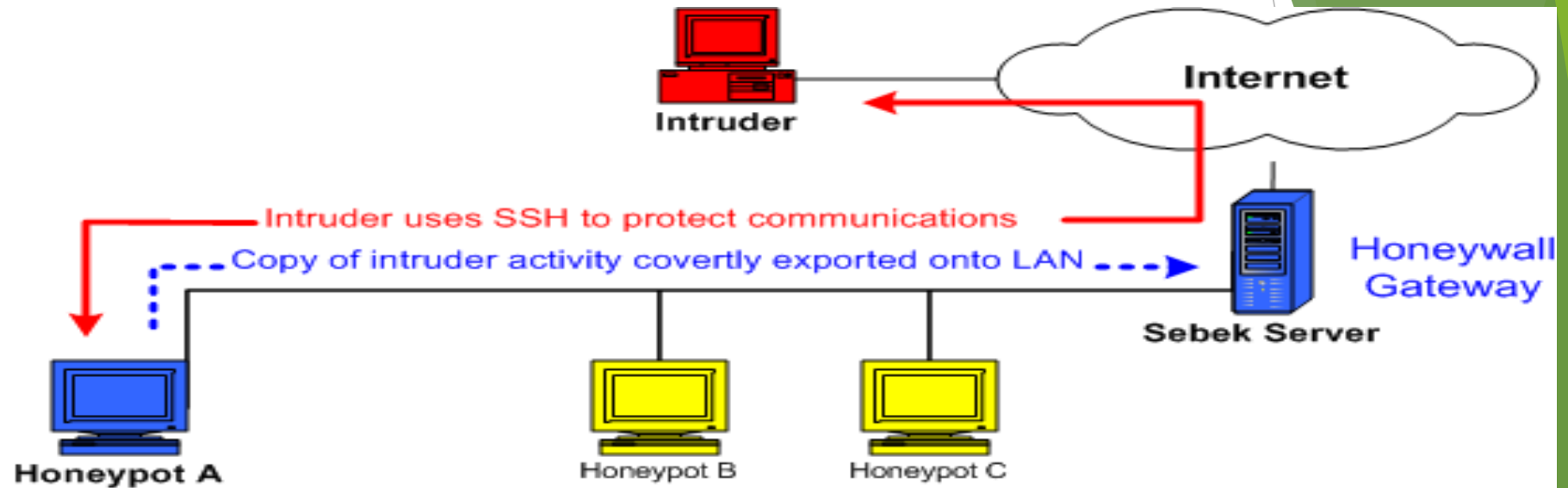
Proyek Honeynet

- ▶ Sebek
- ▶ Honeywall CDRM
- ▶ the Ghost USB honeypot

Sebek

- Modul kernel tersembunyi yang menangkap semua aktivitas host
- Membuat aktivitas bohongan didalam jaringan.
- Penyerang tidak dapat melakukan sniffing lalu lintas berdasarkan IP dan port tujuan.

Sebek Arsitektur



| Time | Protocol | Source IP | Source Port | Destination IP | Destination Port | Service |
|---------------------|----------|-----------------|-------------|----------------|------------------|------------------------------|
| 2003-01-18 15:33:36 | TCP | 212.71.39.18 | 1512 | 10.1.1.101 | 1433 | view, pOf, ARIN (264) |
| 2003-01-18 15:33:37 | TCP | 212.71.39.18 | 1512 | 10.1.1.101 | 1433 | view, pOf, ARIN (264) |
| 2003-01-18 15:42:13 | TCP | 202.107.52.170 | 34777 | 10.1.1.101 | 21 | view, pOf, ARIN (512) |
| 2003-01-18 15:42:13 | TCP | 10.1.1.101 | 1026 | 202.107.52.170 | 113 | view, ARIN (100) |
| 2003-01-18 15:45:18 | TCP | 202.107.52.170 | 53764 | 10.1.1.101 | 21 | view, pOf, ARIN (604) |
| 2003-01-18 15:45:18 | TCP | 10.1.1.101 | 1027 | 202.107.52.170 | 113 | view, ARIN (100) |
| 2003-01-18 15:47:04 | TCP | 202.107.52.170 | 53996 | 10.1.1.101 | 21 | view, pOf, ARIN, Snort (15k) |
| 2003-01-18 15:47:05 | TCP | 10.1.1.101 | 1028 | 202.107.52.170 | 113 | view, ARIN (100) |
| 2003-01-18 15:50:41 | TCP | 202.107.52.170 | 54018 | 10.1.1.101 | 21 | view, pOf, ARIN, Snort (16k) |
| 2003-01-18 15:50:42 | TCP | 10.1.1.101 | 1029 | 202.107.52.170 | 113 | view, ARIN (100) |
| 2003-01-18 15:52:16 | TCP | 62.99.207.73 | 3068 | 10.1.1.101 | 80 | view, pOf, ARIN, plugin (9k) |
| 2003-01-18 15:53:28 | TCP | 202.162.193.147 | 61115 | 10.1.1.101 | 22 | view, pOf, ARIN (55k) |
| 2003-01-18 15:54:46 | TCP | 10.1.1.101 | 1030 | 212.15.64.41 | 80 | view, ARIN, plugin (522k) |
| 2003-01-18 15:54:46 | ICMP | 10.14.0.20 | 0 | 10.1.1.101 | 0 | view, ARIN (0) |
| 2003-01-18 15:55:37 | ICMP | 10.14.0.20 | 0 | 10.1.1.101 | 0 | view, ARIN (0) |
| 2003-01-18 15:56:34 | TCP | 10.1.1.101 | 1031 | 205.158.62.27 | 25 | view, ARIN (1k) |
| 2003-01-18 15:57:35 | UDP | 64.56.227.36 | 1026 | 10.1.1.101 | 137 | view, ARIN (78) |
| 2003-01-18 15:58:31 | TCP | 202.162.193.147 | 61202 | 10.1.1.101 | 1981 | view, pOf, ARIN (65k) |
| 2003-01-18 16:00:02 | TCP | 63.197.22.179 | 3237 | 10.1.1.101 | 1433 | view, pOf, ARIN (264) |
| 2003-01-18 16:00:03 | TCP | 63.197.22.179 | 3237 | 10.1.1.101 | 1433 | view, pOf, ARIN (264) |
| 2003-01-18 16:00:03 | TCP | 63.197.22.179 | 3237 | 10.1.1.101 | 1433 | view, pOf, ARIN (264) |
| 2003-01-18 16:04:11 | TCP | 10.1.1.101 | 1032 | 66.78.27.2 | 80 | view, ARIN, plugin (1m) |
| 2003-01-18 16:05:49 | TCP | 202.107.52.170 | 34999 | 10.1.1.101 | 21 | view, pOf, ARIN (977) |
| 2003-01-18 16:05:49 | TCP | 10.1.1.101 | 1033 | 202.107.52.170 | 113 | view, ARIN (100) |

| Sebek | | | | | | |
|--|-----------|------|------|----------|----|--|
| Home Keystrokes Browse Search | | | | | | |
| Keystroke Summary View for IP: 10.0.1.13 | | | | | | |
| Details | IP | PID | UID | COMMAND | FD | DATA |
| | 10.0.1.13 | 1318 | 0 | sh | 0 | [2003-07-23 20:04:33]# ls [2003-07-23 20:04:34]# less messages [2003-07-23 20:04:52]# cd /etc [2003-07-23 20:04:54]# mkdir ... [2003-07-23 20:04:57]# ls |
| | 10.0.1.13 | 1323 | 0 | less | 3 | [2003-07-23 20:04:35]# v000 [2003-07-23 20:04:50]# q |
| | 10.0.1.13 | 1321 | 0 | w | 6 | [2003-07-23 20:04:09]# w000 |
| | 10.0.1.13 | 1271 | 500 | bash | 0 | [2003-07-23 20:03:29]# ho[BS] [BS] who [2003-07-23 20:03:33]# vv [2003-07-23 20:03:43]# ./malware [2003-07-23 20:03:47]# chmod u[BS] +x mal [2003-07-23 20:03:52]# ./mal |
| | 10.0.1.13 | 1312 | 500 | w | 6 | [2003-07-23 20:03:33]# w000 |
| | 10.0.1.13 | 1271 | 500 | bash | 3 | [2003-07-23 20:03:24]# [BS] [BS] |
| | 10.0.1.13 | 1304 | 500 | tput | 3 | [2003-07-23 20:03:24]# v000 |
| | 10.0.1.13 | 1305 | 500 | wc | 0 | [2003-07-23 20:03:24]# [BS] |
| | 10.0.1.13 | 1307 | 500 | tput | 3 | [2003-07-23 20:03:24]# v000 |
| | 10.0.1.13 | 1302 | 500 | tput | 3 | [2003-07-23 20:03:24]# v000 |
| | 10.0.1.13 | 1252 | 0 | mingetty | 0 | [2003-07-23 20:03:16]# blackhat |
| | 10.0.1.13 | 1263 | 0 | sshd | 7 | [2003-07-23 20:02:07]# v000v000v000 |
| | 10.0.1.13 | 1264 | 500 | scp | 0 | [2003-07-23 20:02:07]# C0664 38802 malware [2003-07-23 20:02:09]# v000 |
| | 10.0.1.13 | 1263 | 0 | sshd | 3 | [2003-07-23 20:02:09]# v000 |
| | 10.0.1.13 | 0 | sshd | 4 | 4 | [2003-07-23 20:02:02]# SSH-2.0-OpenSSH_3.1p1 |

Roo Honeywall CDROOM

- Berdasarkan Fedora Core
- Perangkat keras dan dukungan internasional yang jauh lebih baik.
- Instalasi otomatis
- Antarmuka Walleye baru untuk administrasi berbasis web dan analisis data.
- Pembaruan sistem otomatis.

Instalasi

- Cukup masukkan CDROM dan boot, itu menginstal ke hard drive lokal.
- Setelah reboot untuk pertama kalinya, ia menjalankan skrip berdasarkan standar keamanan NIST dan CIS.
- Setelah instalasi, Anda mendapatkan prompt perintah dan sistem siap dikonfigurasi.

the Ghost USB honeypot

- ▶ Ghost adalah honeypot untuk malware yang menyebar melalui perangkat penyimpanan USB.
- ▶ Mendeteksi infeksi dengan malware semacam itu tanpa memerlukan informasi lebih lanjut

Network Teleskop

- Juga dikenal sebagai **darknet**, **Internet motion sensor** atau **Black hole**.
- Memungkinkan seseorang untuk mengamati berbagai peristiwa berskala besar yang terjadi di Internet.
- Ide dasarnya adalah mengamati lalu lintas yang menargetkan ruang alamat jaringan yang tidak terpakai.
- Karena semua lalu lintas ke alamat ini mencurigakan, seseorang dapat memperoleh informasi tentang kemungkinan serangan jaringan
 - ✓ Worm, dan backscatter DDoS
- Serta misconfigurations lainnya dengan mengamatinya.

Honeytaken

- honeytokens adalah honeypots yang bukan sistem komputer.
- Nilai mereka tidak terletak pada penggunaannya, tetapi dalam penyalahgunaannya.
- Dengan demikian, mereka adalah generalisasi dari ide-ide seperti honeypot.
- Secara umum, Honeytaken tidak selalu mencegah gangguan data Contoh honeytoken adalah alamat email palsu yang digunakan untuk melacak email yang diambil .
- Honeytokens bisa ada di hampir semua bentuk,
 - ✓ Account palsu
 - ✓ Data Palsu,
 - ✓ membuat konsep ini ideal untuk memastikan integritas data.

Terimakasih