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 menggumpilkan 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 honepot.
- 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

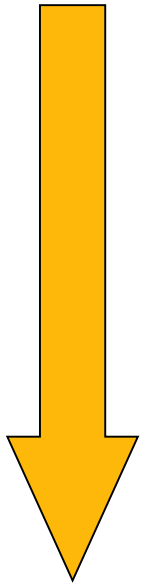
Research

- 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

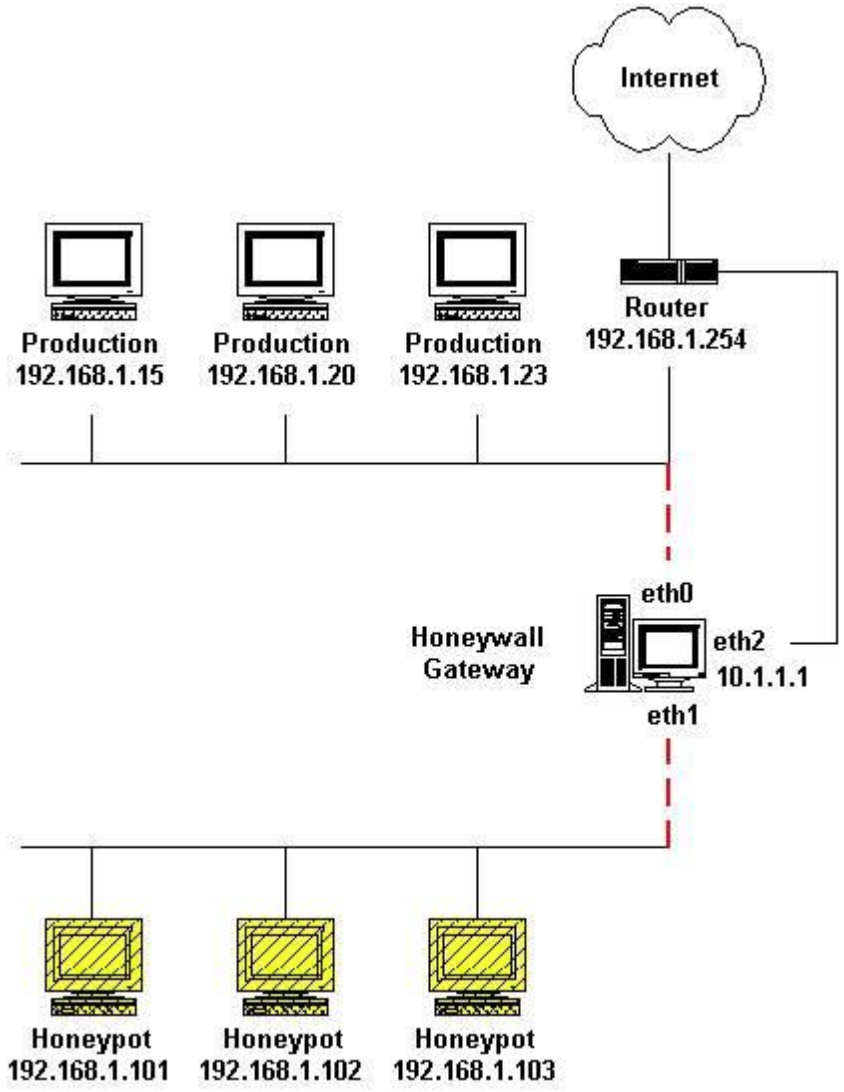
Honeynet

- High-interaction Honeypot dirancang untuk menangkap informasi mendalam.
- Ini adalah arsitektur yang 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

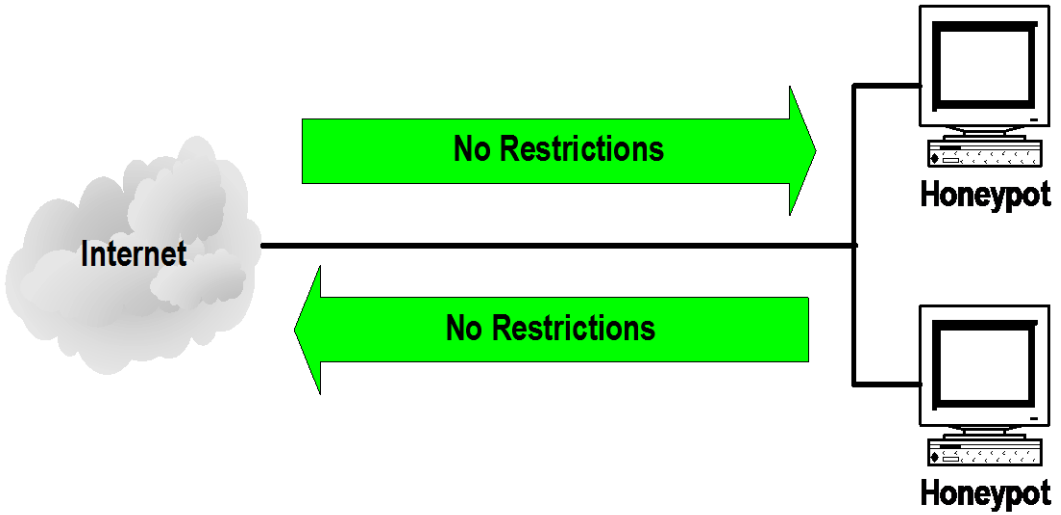
Arsitektur Honeynet



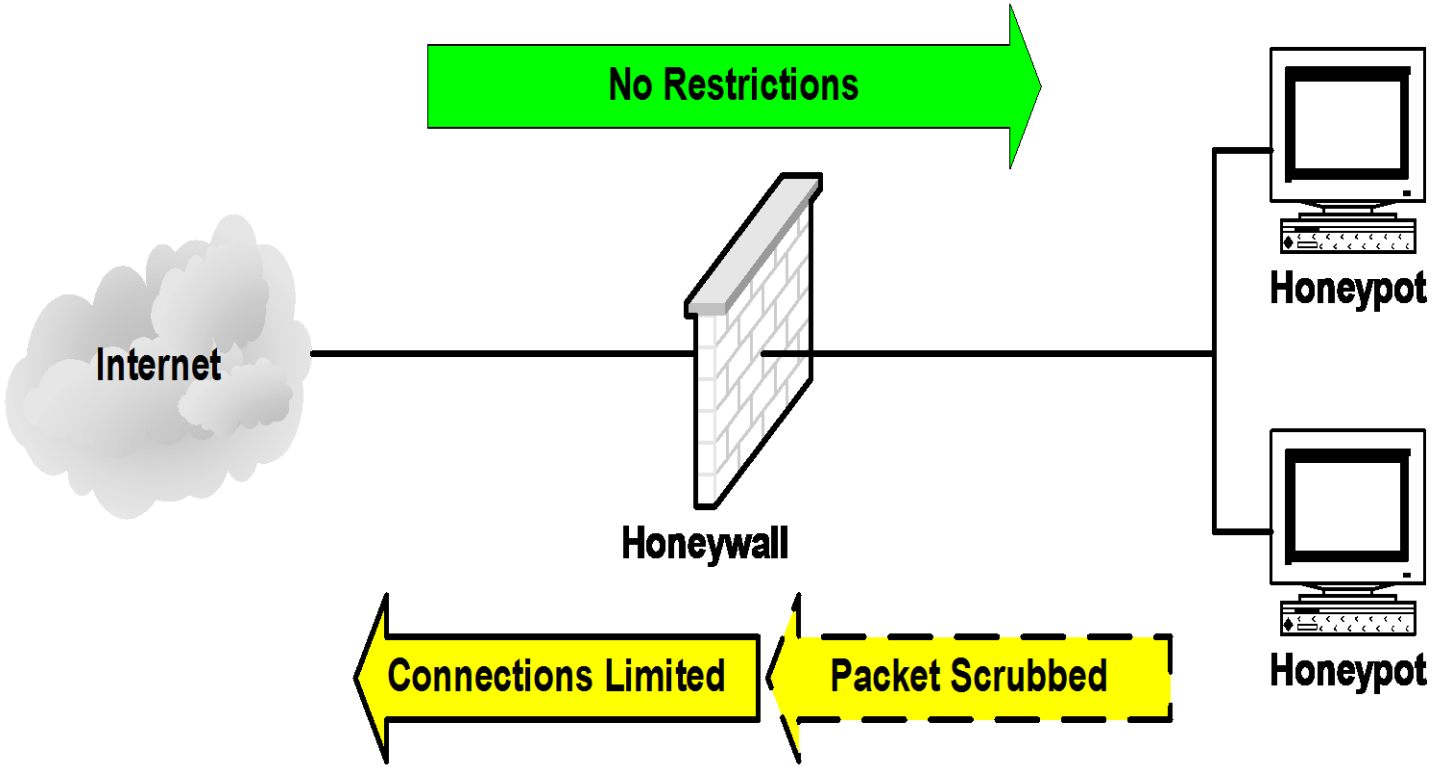
Kontrol Data

- Memitigasi risiko honeynet yang digunakan yang dapatmerusak 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.

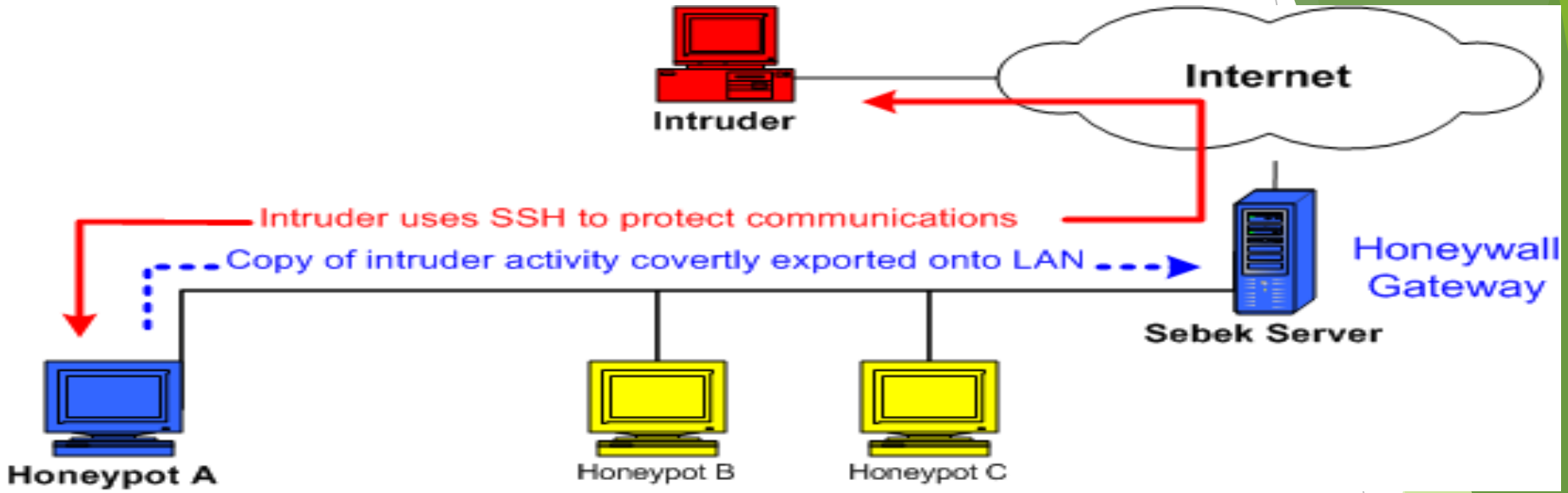
Proyek Honeynet

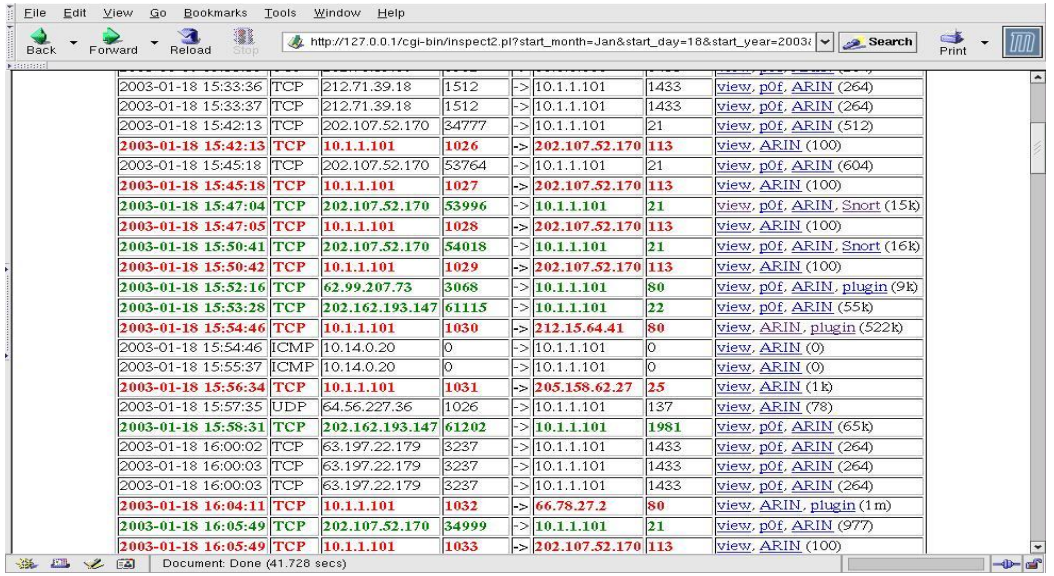
- Sebek
- Honeywall CDROM
- the Ghost USB honeypot

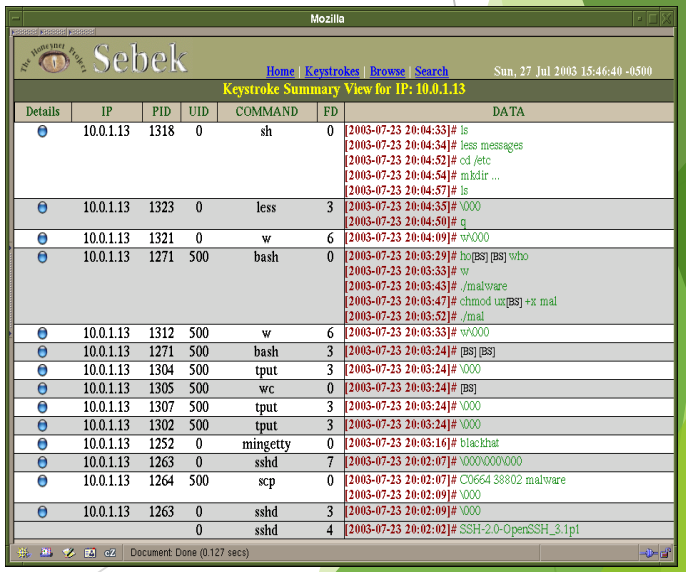
Sebek

- 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







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.

Installasi

- 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