Utilisation des outils Honeypot pour la détection d'intrusion

De la corrélation des événements réseau et système...

Philippe BIONDI — Cédric BLANCHER

philippe.biondi@eads.net / cedric.blancher@eads.net
Centre Commun de Recherche
Département SSI
Suresnes, FRANCE

Eurosec
22 mars 2005

EADS CCR

Plan

EADS CCR

Outils

Les outils usuellement utilisés :

- Sondes réseau
- Sondes système
- Systèmes d'aggrégation, consolidation, corrélation

Limitations

- Ces outils ne couvrent pas la globalité des événements
- Les événements ne sont pas liés entre eux
- La corrélation est très difficile à automatiser

L'analyse et la qualification d'une succession d'événement demande un travail humain long et méticuleux.

Plan

EADS CCR

Honeypot

Définition :

- Un *honeypot* est un système d'information dont la valeur réside dans sa compromission

Trois but possibles

- **Paratonerre** : protection des autres machines grâce à une machine plus attirante
- **Canari** : machine représentative du SI mais observée de près pour déduire l'état du SI.
- **Recherche** : observation des pirates, de leurs outils et de leurs méthodes

Plan

EADS CCR

Mise en œuvre d'un honeypot

La mise en œuvre d'un honeypot suppose un système de surveillance :

- Événements réseau
- Événements système
- Centralisation
- Consolidation
- Corrélation

Plan

EADS CCR

Lien avec la détection d'intrusion

Nous allons utiliser les outils du monde des *honeypots* dans un but de détection d'intrusion.

Plan

EADS CCR

Surveillance

Sur un honeypot, toutes les ressources sont surveillées :

- Réseau : capture et analyse de trafic, sondes IDS
- Système : analyse de logs, outils de surveillance en profondeur, sondes IDS

La couverture d'un honeypot est large, comparée à un IDS sur un SI de production

Plan

EADS CCR

Outils utilisés

Les outils développés par le Honeynet Project[HNEY]

- `Sebek` : surveillance système
- `Hflow` : surveillance des flux réseau
- `Walleye` : consultation des informations

Sebek v2.2

Sebek surveille le système par interception d'appels systèmes

- Création de processus
- Activité des processus
- Données échangées et traitées
- Nouveau : informations réseau (sockets)

Sebek nous donne une vision (presque) complète de l'activité du système, suspicieuse ou non

EADS CCR

Hflow

`Hflow` traite une analyse de flux au format Netflow

- Identification des participants
- Identification des jeux de ports
- Quantité de données échangées

L'analyse par flux est plus pertinente que l'analyse par paquet pour reconstituer les échanges réseau d'une machine

Walleye

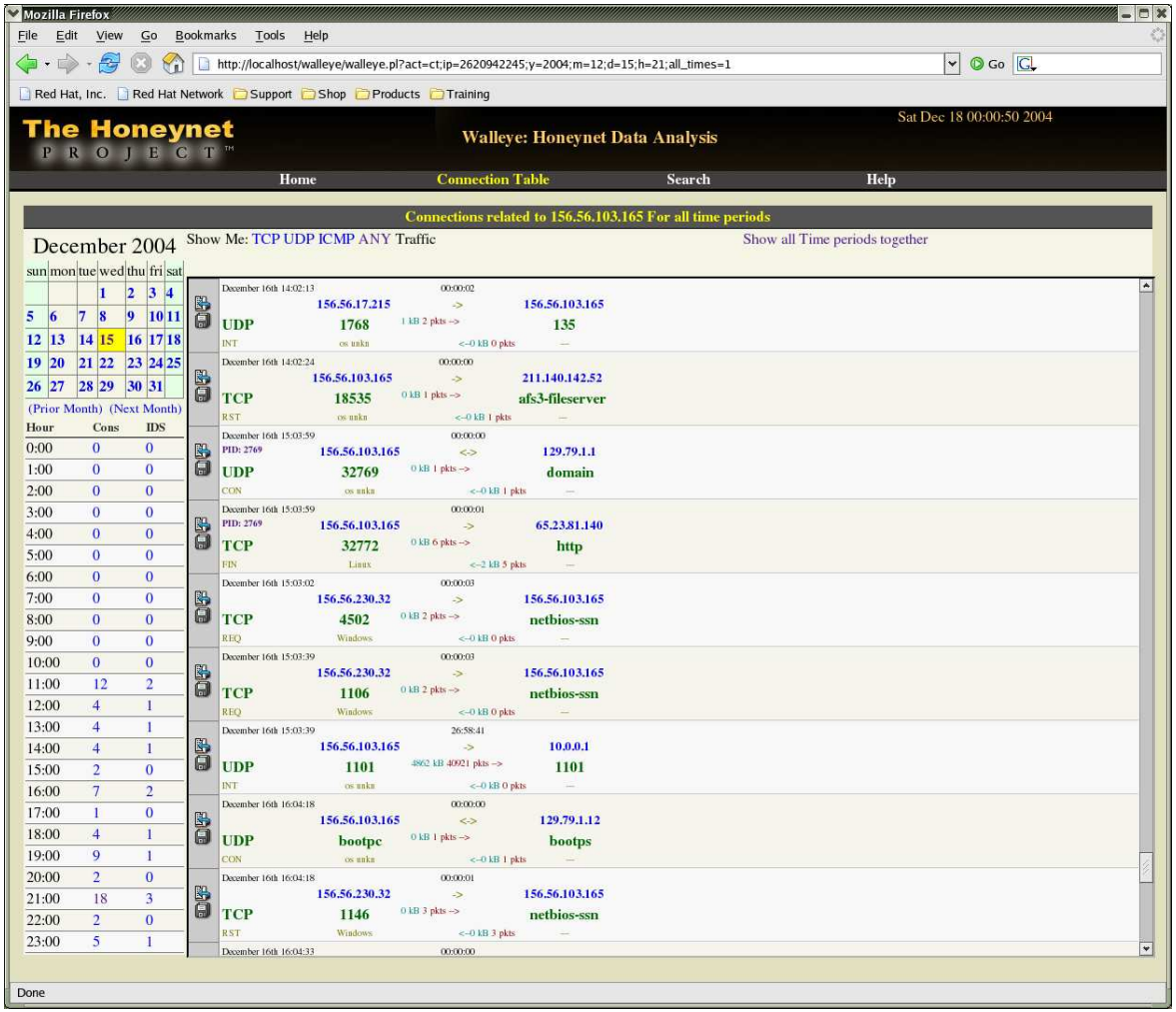
Interface de consultation Sebek+Hflow

- Visualisation des flux réseau
- Visualisation des événements systèmes
- Nouveau : corrélation réseau/système

EADS CCR

Walleye : exemple

Suivi d'un flux réseau et des processus associés

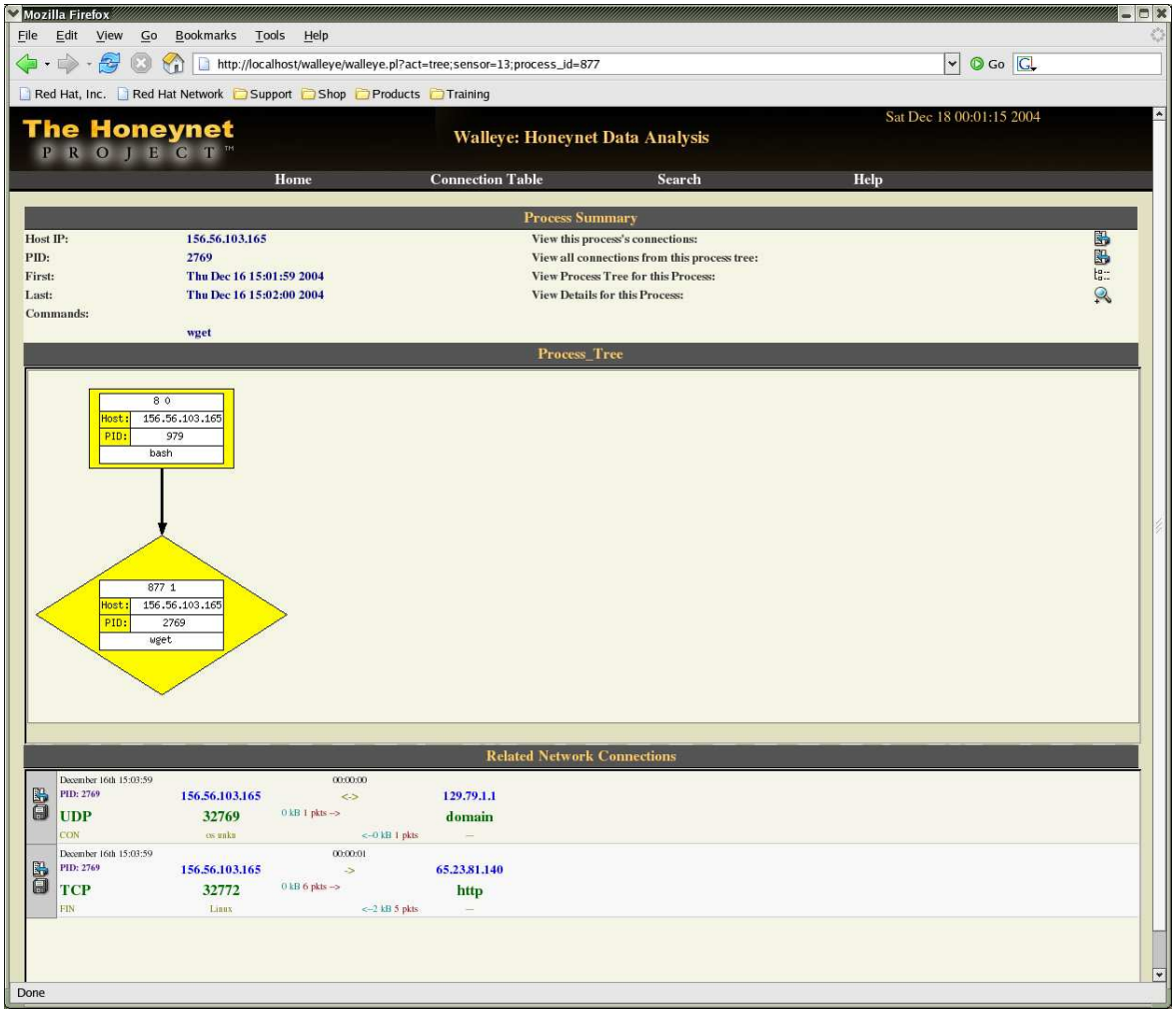


Walleye : exemple

Suivi d'un flux réseau et des processus associés

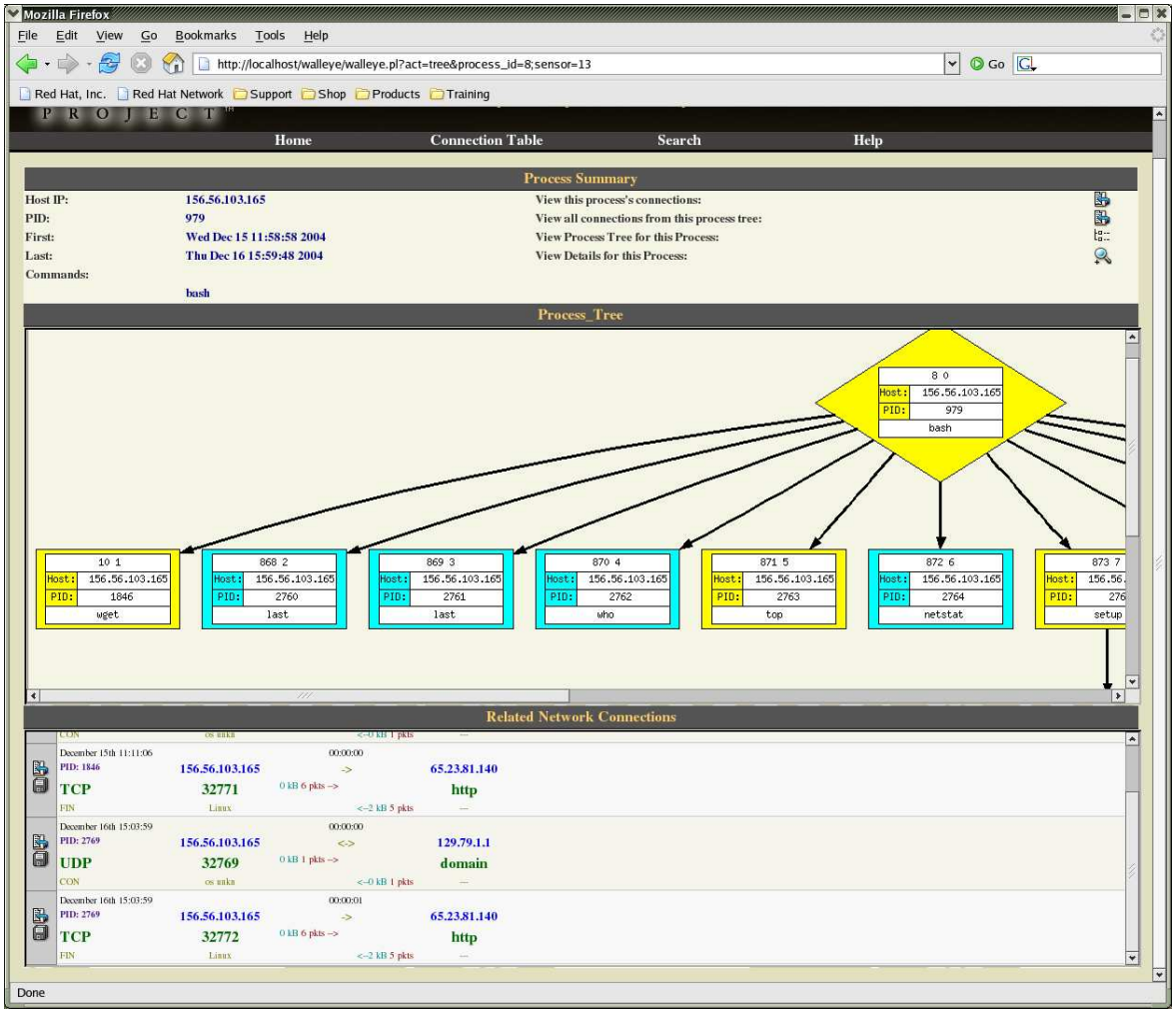
Walleye : exemple

Suivi d'un flux réseau et des processus associés



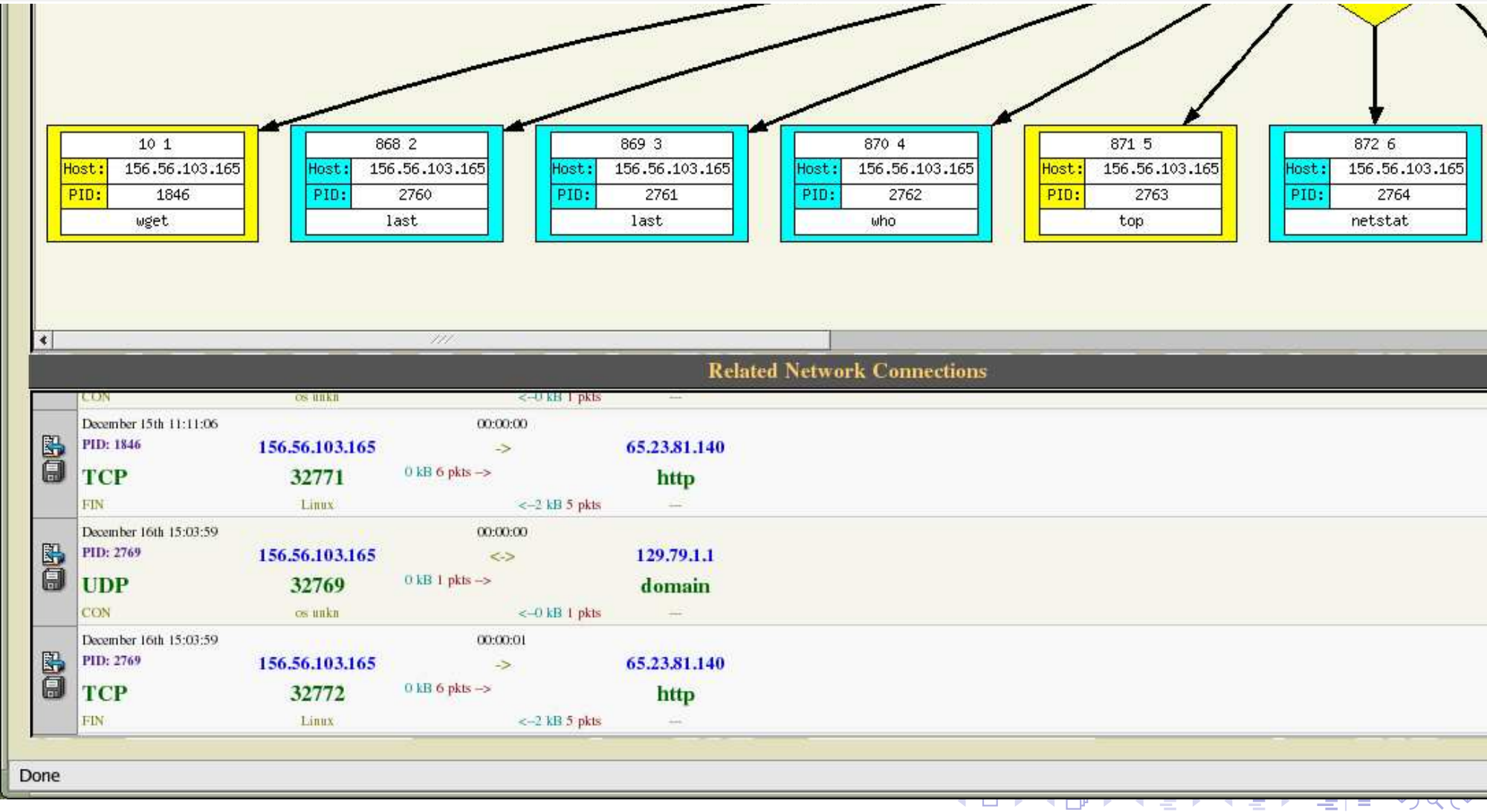
Walleye : exemple

Suivi d'un flux réseau et des processus associés



Walleye : exemple

Suivi d'un flux réseau et des processus associés



Plan

So what ?

Nous sommes capable, à partir d'un flux réseau, de retrouver la suite de l'échange

- Le processus généré par le flux sur la machine destination
- L'arbre de processus généré
- Les connexions réseaux initiées par les processus identifiés
- Etc.

Ces tâches sont, dans une certaines mesure, automatisables

Plan

EADS CCR

Comment qualifier ?

La qualification des alertes est un point crucial. Il s'agit de pouvoir répondre aux questions :

- L'alerte est-elle réelle ?
- Est-ce que l'attaque est pertinente ?
- Est-ce que l'attaque a réussi ?
- Est-ce que l'intrus peut escalader ?
- Etc.

Besoin fort de corrélation

Qualification

Grâce à une base type `Sebek+Hflow`, nous pouvons qualifier une alerte en analysant son contexte :

- Source, destination, type d'attaque, etc.
- Réaction de la cible
- Événements précédents
- Événements immédiats liés

L'idée est de fournir à l'opérateur une qualification pertinente en fonction du contexte.

Plan

EADS CCR

Vers un IDS globalisé

La détection d'intrusion doit tenir compte de tous les événements
L'IDS est réparti sur l'ensemble du SI

Plan

EADS CCR

Corrélation

Corrélation avec les événements pour qualifier l'alerte.

- Est-ce que le flux qui contenait l'attaque a généré un process ?
- Quel type de process a été généré ?
- Qu'a fait le process ?
- Etc...

Bibliographie I

 Honeyney Project http://www.honeynet.org/