

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



Plan

- 1 De la détection d'intrusion
- 2 Honeypots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honeypot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

- 1 De la détection d'intrusion
- 2 **Honeypots**
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honeypot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

Honeypot

Définition :

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

Trois but possibles

- **Paratonnerre** : 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

- 1 De la détection d'intrusion
- 2 **Honeypots**
 - Définition
 - **Mise en œuvre**
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honeypot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

- 1 De la détection d'intrusion
- 2 **Honeypots**
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honeypot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

Lien avec la détection d'intrusion

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

Plan

- 1 De la détection d'intrusion
- 2 Honey pots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honey pot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

- 1 De la détection d'intrusion
- 2 Honeybots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honeybot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

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

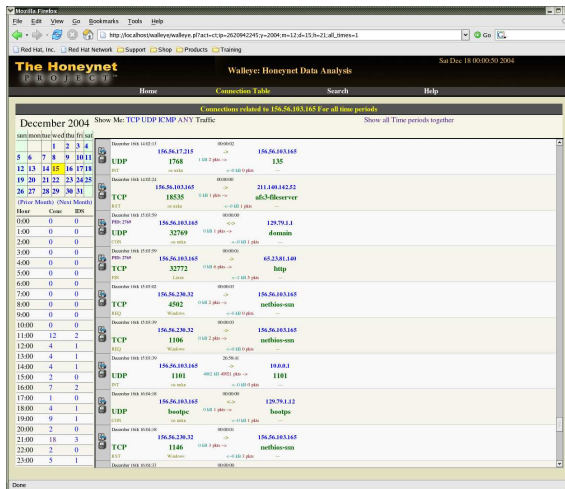
Walleye

Interface de consultation Sebek+Hflow

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

Walleye : exemple

Suivi d'un flux réseau et des processus associés



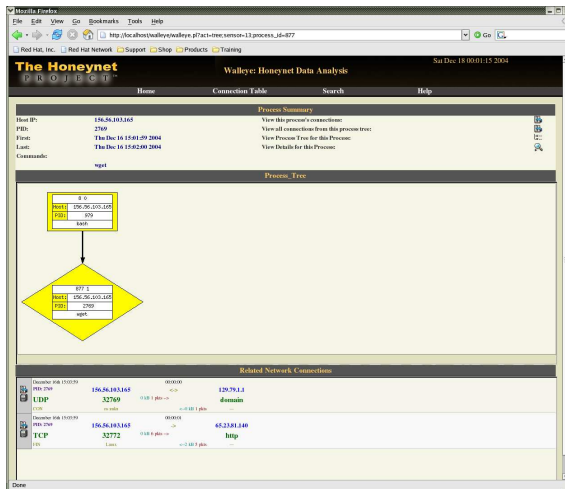
Walleye : exemple

Suivi d'un flux réseau et des processus associés

nth) S		TCP	18535	0 kB 1 pkts →	afs3-filer
		RST	os unkn	←-0 kB 1 pkts	—
		December 16th 15:03:59		00:00:00	
		PID: 2769	156.56.103.165	↔	129.79.1.1
		UDP	32769	0 kB 1 pkts →	domain
		CON	os unkn	←-0 kB 1 pkts	—
		December 16th 15:03:59		00:00:01	
		PID: 2769	156.56.103.165	→	65.23.81.140
		TCP	32772	0 kB 6 pkts →	http
		FIN	Linux	←-2 kB 5 pkts	—
		December 16th 15:03:02		00:00:03	
			156.56.230.32	→	156.56.103.165
		TCP	4502	0 kB 2 pkts →	netbios-ssn
		REQ	Windows	←-0 kB 0 pkts	—

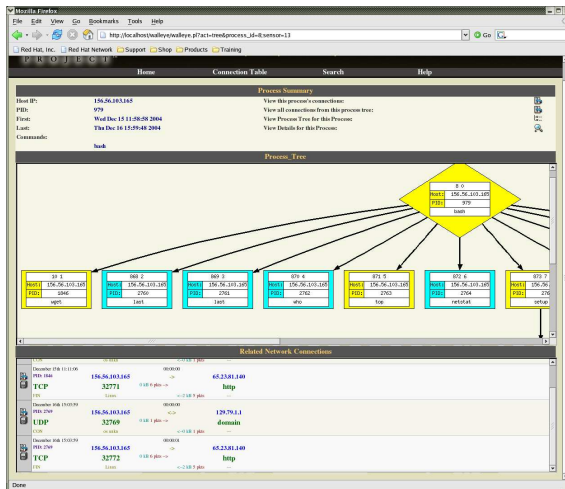
Walleye : exemple

Suivi d'un flux réseau et des processus associés



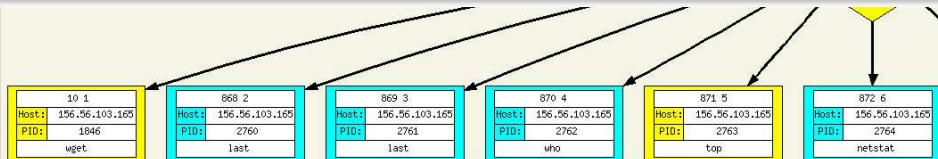
Walleye : exemple

Suivi d'un flux réseau et des processus associés



Walleye : exemple

Suivi d'un flux réseau et des processus associés



Related Network Connections					
CON	os unka	<-0 kB 1 pkts	--		
December 15th 11:11:06		00:00:00			
PID: 1846	156.56.103.165	->	65.2381.140		
TCP	32771	0 kB 6 pkts ->	http		
FIN	Linux	<-2 kB 5 pkts	--		
December 16th 15:03:59		00:00:00			
PID: 2769	156.56.103.165	<->	129.79.1.1		
UDP	32769	0 kB 1 pkts ->	domain		
CON	os unka	<-0 kB 1 pkts	--		
December 16th 15:03:59		00:00:01			
PID: 2769	156.56.103.165	->	65.2381.140		
TCP	32772	0 kB 6 pkts ->	http		
FIN	Linux	<-2 kB 5 pkts	--		

Plan

- 1 De la détection d'intrusion
- 2 Honey pots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honey pot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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 certaine mesure, automatisables

Plan

- 1 De la détection d'intrusion
- 2 Honey pots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honey pot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

- 1 De la détection d'intrusion
- 2 Honey pots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honey pot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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

- 1 De la détection d'intrusion
- 2 Honey pots
 - Définition
 - Mise en œuvre
 - Liens avec la détection d'intrusion
- 3 Outils de surveillance Honey pot
 - La surveillance
 - Outils
 - Conclusion
- 4 Application aux IDS
 - Qualification
 - Globalisation
 - Corrélation

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/>