



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

**Flux réseaux :
Analyse après compromission
d'un pot de miel**

OSSIR - Mars 2004

Yann Berthier - FHP

<yb@hsc.fr>

- x Pot de miel compromis en Septembre 2003
 - x Pas de connaissance a priori de l'environnement
 - x Analyse menée en parallèle à l'analyse «système» (log Sebek)
- x 24 heures de capture
 - x de 01:02:54 le 12/09/03 à 01:01:03 le 13/09
- x Trace au format pcap de 19 Mo
- x 192700 paquets
- x 19679 yb -20 5 148M 13M swread 417:01 69.53% 69.53% ethereal

Où il est question de flux réseau en général,
et de Argus en particulier ...

- x Historiquement, utilisés par les ISP
 - x Facturation / comptabilité
 - x DoS
- x Outils matures
- x Outils adaptés pour gérer du trafic
- x Au niveau des équipements de routage / commutation
 - x Cisco : NetFlow
(<http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml>)

Définition générique d'un flux

- x «Ensemble de paquets possédant des caractéristiques communes»
 - x Adresses IP source et destination
 - x Protocole
 - x Ports source (quand applicable)
 - x Port destination (quand applicable)
 - x Début du flux
 - x Fin du flux
 - x Autre
 - x Labels MPLS, numero d'AS, ...

Génération de flux réseaux

- x Sur les routeurs
- x Avec une sonde (PC, autre) qui écoute le trafic
 - x Argus (<http://qosient.com/argus/>)
 - x Nprobe (<http://www.ntop.org/nProbe.html>)
 - x Fprobe (<http://fprobe.sourceforge.net/>)
 - x ng_netflow (<http://cell.sick.ru/~glebius/>)
- x En cours de normalisation à l'IETF
 - x groupe de travail IPFIX
 - x Basé sur Cisco NetFlow v9

Exploitation des flux

- x Argus (ra*)
 - x A partir de données au format Argus
 - x A partir de données NetFlow
- x Flow-tools (<http://www.splintered.net/sw/flow-tools/>)
- x Cflowd (<http://www.caida.org/tools/measurement/cflowd/>)
- x Rrdtool (<http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>)
- x Netams (<http://www.netams.com/>)
- x Flowc (<http://netacad.kiev.ua/flowc/>)

Argus – définitions d'un flux

- x Bi-directionnel
- x Couple (saddr, sport), (daddr, dport)
- x Nombre de paquets et d'octets du flux (in/out)
- x Durée du flux (date de début, date de fin)
- x Données exportées toutes les x minutes (même si flux en cours)
- x Gestion des états
 - x TCP
 - x Flux commence avec le premier SYN
 - x S'arrête avec un FIN ou un RST
 - x Délai d'expiration (timeout)
 - x Conservation des états : RST, FIN, TIM, ACC

- x **Serveur Argus**

- x Prend des données pcap
- x Génère des flux au format Argus

- x **Clients Argus**

- x ra
- x ragator : agrégation des flux
- x ramon : rapports de type RMON2 après agrégation et tri
 - x Matrix : liste des «conversations»
 - x TopN
 - x Svc : liste des ports destination
 - x HostSvc : liste des adresses sources par port destination

- x **Exemple de sortie de ragator**

12 Sep 03 05:50:34 7199 6 xx.xx.xx.xx.4290 -> 172.16.134.101.139 2 2 128 140 RST

Autopsie d'une trace réseau

- x Mise en évidence des flux significatifs
 - x Flux de longue durée
 - x Grand nombre d'octets – en source ou en destination
 - x Grand nombre de flux d'une adresse source vers une adresse / un sous-réseau (scan)
 - x **Flux émis depuis le honeypot !**
- x Reconstitution d'une timeline autour de ces évènements
- x Outils
 - x Argus : ra, ragator, ramon
 - x Grep / cut / sort / head / uniq

24 heures de la vie d'un pot de miel

- x Début de trace : 01:02:54 le 12/09
- x Activité constatée dans la trace
 - x 80/TCP, 135/TCP, 139/TCP, 445/TCP, 1434/UDP
- x Pas possible de distinguer le bruit d'un éventuel «scan de reconnaissance»
- x Des flux non pertinents

01:02:54 85685 17 172.16.134.101.138 -> 172.16.134.127.138 238 0 60095 0 INT

01:32:48 79787 17 172.16.134.101.1101-> 10.0.0.1.1101 1825 0 172301 0 INT

- x Des flux manquants
 - x **Pas** de flux de résolution dans la trace !

- × Plusieurs flux sur le port 139/TCP depuis une adresse dans la zone APNIC (Taiwan)

05:44:21	1	6	xx.xx.84.30.42222	->	172.16.134.101.139	4	3	272	206	FIN
05:50:31	1	6	xx.xx.84.30.42254	->	172.16.134.101.139	2	2	4649	542	RST
05:50:32	1	6	xx.xx.84.30.42882	->	172.16.134.101.139	8	8	4649	612	RST
05:50:32	1	6	xx.xx.84.30.42883	->	172.16.134.101.139	8	7	4649	546	RST

- × Des flux sur le port 45295 depuis cette même adresse

05:50:33	0	6	xx.xx.84.30.42899	->	172.16.134.101.45295	1	1	74	54	RST
05:50:34	0	6	xx.xx.84.30.42902	->	172.16.134.101.45295	1	1	74	54	RST
05:50:37	0	6	xx.xx.84.30.42938	->	172.16.134.101.45295	3	2	198	132	FIN
05:50:37	0	6	xx.xx.84.30.42939	->	172.16.134.101.45295	2	2	132	132	FIN

- * A partir de 15:29:53, plusieurs flux depuis une **autre** adresse sur le port 45295
 - * Sans scan préalable

15:29:57 219 6 xxx.xx.106.90.1905 -> 172.16.134.101.45295 32 33 2201 9996 FIN

```
% whois xxx.xx.106.90
```

```
OrgName: Latin American and Caribbean IP address Regional Registry
```

```
OrgID: LACNIC
```

```
Address: Potosi 1517
```

```
City: Montevideo
```

* A partir de 15:30

15:30:43 7 6 172.16.134.101.1035 -> xxx.xxx.153.133.80 198 366 13288 546916 FIN

15:31:48 3 6 172.16.134.101.1039 -> xx.xxx.103.248.25 12 8 966 981 FIN

15:31:48 47 6 172.16.134.101.1040 -> xxx.xx.230.37.25 14 7 1118 667 FIN

* xxx.xxx.153.133 résout en www.<blah>.ro

- × A 15:32, flux depuis une troisième adresse sur le port 50/TCP
 - × Sans scan préalable

15:32:16 5152 6 xxx.xx.42.162.1542 -> 172.16.134.101.50 871 913 58414 199049 RST

inetnum: xxx.xx.42.0 - xxx.xx.43.255

netname: XXXXXXXX-PI-RE-RO-TERRASAT

descr: XXXXXXXX ISP, Moldova Noua, RO

x 15:40 : Serveur en Roumanie

15:40:19 1 6 172.16.134.101.1042 -> xxx.xxx.111.13.21 3 3 206 206 FIN

15:40:36 3 6 172.16.134.101.1043 -> xxx.xxx.111.13.21 3 3 206 206 FIN

x 15:41:03 : Serveur en Suède

15:41:03 182 6 172.16.134.101.1044 -> xx.xxx.20.133.21 39 29 2362 2360 FIN

15:42:26 1 6 172.16.134.101.1045 -> xx.xxx.20.133.28395 4 4 236 1419 FIN

15:42:49 19 6 172.16.134.101.1046 -> xx.xxx.20.133.29589 164 232 8876 324720 FIN

15:43:50 3 6 172.16.134.101.1047 -> xx.xxx.20.133.25597 38 44 2072 56068 FIN

15:43:58 1 6 172.16.134.101.1048 -> xx.xxx.20.133.29850 22 22 1208 27116 FIN

x 16:19:37, 23:20:57, 23:34:36 : FTP sur notre premier serveur

- x Dès 16:06:35, flux IRC, **longs**, vers plusieurs serveurs

- x Undernet

16:06:35 32060 6 172.16.134.101.1049 -> xxx.xx.220.2.6667 7493 4882 534795 730680

16:57:21 29020 6 172.16.134.101.2693 -> xxx.xx.102.4.6667 1597 1337 108360 216219

17:09:14 28303 6 172.16.134.101.2705 -> xx.xx.96.42.6667 7833 7834 523879 1223461

- x En parallèle, nombreux flux depuis des adresses (en Roumanie) sur le port 31337, de 16:04 à la fin de la trace

- x Bouncer IRC

- × A partir de 16:12, scans lancés depuis notre pot de miel ...

- × Pas de discretion qui tienne !

De 16:12:49 à 16:18:49 sur xx.130/16 port 139/TCP (10868 scans)

De 16:21:36 à 16:28:18 sur xxx.71/16 port 139/TCP (18153 scans)

De 16:28:22 à 16:35:02 sur xxx.72/16 port 139/TCP (18849 scans)

De 16:35:10 à 16:41:46 sur xxx.73/16 port 139/TCP (19101 scans)

De 16:41:47 à 16:48:30 sur xxx.74/16 port 139/TCP (19036 scans)

De 16:48:31 à 16:55:14 sur xxx.75/16 port 139/TCP (18674 scans)

De 16:55:15 à 16:56:22 sur xxx.76/16 port 139/TCP (3021 scans)

De 19:15:44 à 19:17:04 sur yyy.96/16 port 139/TCP (3888 scans)

De 19:17:13 à 19:18:15 sur zzz.20/16 port 139/TCP (2762 scans)

De 23:24:43 à 23:25:46 sur aaa.20/16 port 22/TCP (3472 scans)

Conclusions

- x L'étude des flux réseau permet de dégager les évènements significatifs
- x En complément de l'analyse système
- x Ce qui passe sur le réseau est **fiable**
 - x Même si difficilement interprétable
- x Nombreux outils existants pour manipuler des flux
- x C'est un processus non automatisé