

I.D.S. : Snort

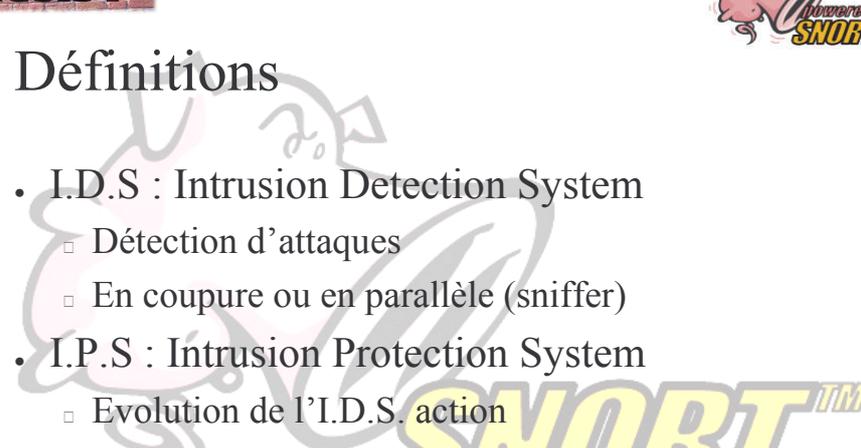
- Définitions
- Snort
- Implémentation
- Conclusions



SNORT™

Définitions

- I.D.S : Intrusion Detection System
 - Détection d'attaques
 - En coupure ou en parallèle (sniffer)
- I.P.S : Intrusion Protection System
 - Evolution de l'I.D.S. action



SNORT™



Snort

- <http://www.snort.org>
- Détecteur d'intrusion Open Source
- Unix et Windows
- Auteurs : Marty Roesch & Brian Caswell

SNORT™



Snort

- Placé en tant que Sniffeur
- Repère des signatures d'attaques
- Repère les scans de ports rapides (redondance avec un FW)

SNORT™

Evolution

- 1.x
 - Version initiale
- 2.0
 - Notion de suppression/seuil de règles
 - Amélioration des suivis de connexion
- 2.1
 - Apparition d'expressions régulières (PCRE) dans les règles

Points forts

- Open Source
- Large communauté d'utilisateurs
 - Beaucoup de contributions
 - Beaucoup de documentations
- Bonne base de signatures
 - Mise à jour
 - Modifiable

Fonctionnement

- Préprocesseurs (avec leur propre ID)
 - defragmenteurs
 - http_inspect
 - rpc_decode, etc.
- Postprocesseurs
 - syslog
 - mysql
 - tcpdump

SNORT™

Règles

format

- type action (alert, + configurable)
- contexte (protocole, origine, destination)
- message
 - contenu, sensibilité à la casse
 - type de flux
 - type d'attaque
 - références (SID, révision, urls, etc.)

SNORT™

Exemple de règle

```
alert tcp $HOME_NET 22 ->  
  $EXTERNAL_NET any (msg:"ATTACK-  
  RESPONSES successful gobbles ssh  
  exploit(GOBBLE)";  
  flow:from_server,established;  
  content:"|2a|GOBBLE|2a|";  
  reference:bugtraq,5093;  
  classtype:successful-admin;  
  sid:1810; rev:3;)
```

Autour de Snort

- Analyse des résultats
- Transformation en I.P.S.

Analyse des résultats

- Acid
- Pigsentry (Temps réel)
- SnortSnarf
- Snortlog (graphiques)

**SNORT™**

Transformation en I.P.S.

- Flexresp (intégrée)
 - bloque une action par TCP/RST
- Snort-inline : modification de snort
 - <http://sourceforge.net/projects/snort-inline/>
- Guardian (ajout de règles iptables)

**SNORT™**



Implémentation à l'UT1

- Placé sur la patte interne du firewall
- Analyse en décalé sur une autre machine
SnortSnarf
- Les difficultés rencontrées
- Repère quelques attaques fines



SnortSnarf

- <http://www.silicondefense.com/software/snortsarf/>
- Présentation Web
- Présentation des signatures détectées
- Présentation des signatures par machine
- Visualisation des paquets fautifs

SnortSnarf

SnortSnarf: Snort signatures in /supplements/snortsnarf/snort.040214070001/alert et al - Mozilla Firefox

SnortSnarf start page
All Snort signatures
SnortSnarf v021111.1

[Signature section \(1328\)](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

1328 alerts found using input module SnortFileInput, with sources:

- /supplements/snortsnarf/snort.040214070001/alert

Earliest alert at 06:31:16 773485 on 02/13/2004
Latest alert at 05:15:55 175970 on 02/14/2004

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
1	WEB-PHP viewtopic.php access [sig]	29	7	1	Summary
1	WEB-CLIENT Outlook EML access [sig]	26	2	5	Summary
1	WEB-ATTACKS rm command attempt [sig]	5	4	1	Summary
1	WEB-PHP PayPal Storefront arbitrary command execution attempt [sig]	1	1	1	Summary
2	WEB-CGI calendar access [sig]	78	29	1	Summary
2	ICMP redirect host [sig]	15	2	3	Summary
2	IMAP login literal buffer overflow attempt [sig]	9	4	1	Summary

SnortSnarf

Summary of alerts in /supplements/snortsnarf/snort.040214070001/alert et al for signature: WEB-ATTACKS rm command attempt - Mozilla Firefox

SnortSnarf signature page
WEB-ATTACKS rm command attempt
SnortSnarf v021111.1

[Signature section \(1328\)](#) [Top 20 source IPs](#) [Top 20 dest IPs](#)

5 alerts with this signature using input module SnortFileInput, with sources:

- /supplements/snortsnarf/snort.040214070001/alert

Earliest such alert at 10:25:55 004975 on 02/13/2004
Latest such alert at 18:22:50 798454 on 02/13/2004

WEB-ATTACKS rm command attempt [4 sources](#) [1 destinations](#)

Priority: 1 Classification: Web Application Attack
[\[sig:1365\]](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
81.50.213.13	2	6	1	1
82.224.8.103	1	4	1	1



SnortSnarf

All 6 alerts from 81.50.213.13 in /supplements/snortsnarf/snort.040214070001/alert et al - Mozilla Firefox

DEFENSE Source: 81.50.213.13

SnortSnarf v021111.1

Signature section (1328) Top 20 source IPs Top 20 dest IPs

6 such alerts found using input module SnortFileInput, with sources:

- /supplements/snortsnarf/snort.040214070001/alert

Earliest 12:35:28 023040 on 02/13/2004
Latest 12:36:34 557849 on 02/13/2004

2 different signatures are present for 81.50.213.13 as a source

- 2 instances of [WEB-ATTACKS rm command attempt](#)
- 4 instances of [\(ftp_inject\) BARF BYTE UNICODE ENCODING](#)

There are 1 distinct destination IPs in the alerts of the type on this page.

81.50.213.13	Whos lookup at:	ARIN	RIPE	APNIC	Geektools
	DNS lookup at:	Amennex	TRIUMF	Princeton	
	More lookup links:	Dnsfield	Sam Spade		

```
02/13-12:35:28.023040 [**] [1:1965:4] WEB-ATTACKS rm command attempt [**] [Classification: Web Application Attack]
Priority: 1 (TCP) 81.50.213.13:1915 -> 193.49.55.209:80 [Snort log]
```



SnortSnarf

Mozilla Firefox

http://syslog.univ-bret.fr/snort.040214070001/log/81.50.213.13/FCP:1915-80

```
[**] WEB-ATTACKS rm command attempt [**]
02/13-12:35:28.023040 81.50.213.13:1915 -> 193.49.55.209:80
TCP TTL:111 TOS:0x00 ID:16584 Iplen:20 Uplen:41 DF
***APP*** Seq: 0xC8B6F716 Ack: 0x715D45A7 Win: 0x3F32 Len: 20
47 45 54 20 2F 73 75 69 6F 2F 65 6D 70 5C 6F 69
73 5F 65 74 75 64 69 61 6E 74 73 2F 76 69 73 75
6C 5F 65 69 70 6C 6F 69 35 70 68 70 3F 69 62 74
69 74 3D 52 65 73 70 6F 6E 73 61 62 6C 65 25 32
30 45 2D 63 72 69 25 32 30 65 74 25 32 3D 62 61
73 65 25 32 3D 64 65 25 32 50 64 6F 6E 6E 69 65
73 26 6E 75 6D 65 72 6F 3D 32 35 37 2D 4B 54 54
50 2F 31 2E 31 0D 0A 41 63 69 65 70 74 3A 2D 2A
2F 2A 0D 0A 7E 7E
7E 3A 7E 7E
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E
0D 0A 41 63 69 65 70 74 2D 4C 61 6E 67 75 61 67
65 3A 2D 66 72 0D 0A 7E 7E 7E 7E 7E 7E 7E
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E
7E 7E 7E 7E 0D 0A 55 73 65 72 2D 41 67 65 6E
74 3A 2D 4B 6F 7A 69 6C 6C 61 2F 34 2E 3D 2D 2B
63 6F 6D 70 61 74 69 62 6C 65 38 2D 4D 53 49 45
2D 36 2E 3D 3B 2D 57 69 6E 64 6F 77 73 2D 4E 54
2D 35 2E 31 2D 0D 0A 4B 6F 73 74 3A 2D 66 6F 72
7E 6D 73 2E 7E 6E 69 76 2D 74 6C 73 65 31 2E 66
72 0D 0A 43 6F 6E 65 63 74 69 6F 6E 3A 2D 4B
65 65 7D 2D 41 6C 69 76 65 0D 0A 0D 0A
...Connection: Keep-Alive...
```

Les difficultés rencontrées

- Les faux positifs
- L'emplacement de la sonde
- La mise à jour (changement des noms de règles)
- Consommation

SNORT™

Les faux positifs

- Règles « inutiles » : ICMP, fingerprinting
 - Difficulté à conserver les renseignements utiles
- Très forte quantité (90%)
 - Analyse fine des applications non présentes
 - Gros travail de régulation et de nettoyage (2.x)
- Mais, les faux persistent (règles trop générales)
- Importance de la présentation des résultats

SNORT™

Limitations des règles I

On peut

- limiter les alertes (threshold type limit)
- détecter sur un seuil (threshold type threshold)
- annuler les règles (suppress)

On peut le faire

- de manière globale (snort.conf)
- dans la définition des règles

On peut préciser

- origine ou la destination (ip ou CIDR)

Limitations des règles II

Seuil

```
threshold gen_id 1, sig_id 448, type limit, track  
by_src, count 1, seconds 300
```

pour une même IP source ICMP Source Quench
pas plus de 1 par 5 minutes

Suppression

```
suppress gen_id 1, sig_id 526, track by_dst, ip  
193.49.48.249
```

pas d'alerte pour la signature 526 pour la
destination 193.49.48.249

L'emplacement de la sonde

- Avant ou après le firewall ?
- Avant :
 - Prévision
 - Analyse comportementale des pirates
- Après :
 - Détection des failles utilisées

La mise à jour des règles

- 2400 règles disponibles
- Plutôt réactif
- Détection de shellcodes
- Tendance des auteurs à changer les noms des règles :-)

Consommation CPU/RAM

- Sonde
 - Pour 500 Ko/seconde
 - 4 % de CPU sur un pentium III à 933Mhz
 - 40-60 Mo de RAM
- Analyse
 - Très consommateur
 - Très fluctuant (>500 Mo de RAM possible)
 - Attention à la résolution DNS

• Consommation disque

- 30 -100 Mo de dump par jour
- 1-10 Mo d'alertes par jour
- 0.5 à 2 Mo de pages Web par jour
- Quelques pointes à 20 Mo de Web

Consommation RSSI

- Lancement
 - 1 journée de paramétrage
 - 30 minutes par jour pendant 15 jours
- Rythme de croisière
 - 5-15 minutes par jour (si correctif)
- Accidents de parcours
 - 3 heures (chgt de règles, attaque imprévue)

Conclusions

- Ne remplace par un firewall
- Permet de
 - Détecter les intrusions
 - Détecter les pirates
- Facile à installer
- Travail long et attentif pour ne pas noyer le RSSI