Administration réseaux - Les systèmes de détection d'intrusion

Julien Bourdon - Julien Legras - Jean-Baptiste Souchal

Master 2 Sécurité des Systèmes Informatiques

17/01/2014

Sommaire

1. Présentation générale
   - Les IDS
   - Les IPS
2. Snort
   - Fonctionnalités
3. Suricata
   - Fonctionnalités
   - Fonctionnalités avancées
4. Snorby
5. Prelude
6. Démonstration
   - Réseau utilisé
   - Attaques & règles de filtrage
7. Conclusion

Les IDS I

Objectifs des IDS

- Surveiller
- Contrôler
- Détecter
- Sniffer & analyser

Domaines d'analyse

- Couche réseau (IP, ICMP)
- Couche transport (TCP, UDP)
- Couche application (HTTP, telnet)

Les IDS II

Types

- HIDS
- NIDS

Actions

- Journaliser
- Avertir (système, humain)
- Agir (fin de connexion...)

Les IDS III

Méhodes de détection

- Signature
  - Expressions régulières
  - Comparaison avec les signatures connues
- Comportementale
  - Détection d'anomalie
  - Vérification d'intégrité

Dangers

- Faux-positifs
- Faux-négatifs

  $\hookrightarrow$ Evasion

Les IPS

Fonctionnalités

- IDS avec fonction de blocage
- Interrompre ou ralentir la connexion
- Blacklister une source
- Attention aux faux-positifs

Introduction

Snort

- IDS le plus utilisé ($\sim$ 2 millions de téléchargements)
- Création en 1998 par Marty Roesh
- Open source
- Association possible avec un pare-feu

Fonctionnalités I

Architecture

- Décodeur de paquets
- Pré-processeurs
- Moteur de détection
- Système d'alerte et d'enregistrement
- Modules de sortie

Fonctionnalités II

Actions en mode IDS

- alert
- log
- pass
- activate
- dynamic

Actions en mode IPS

- drop
- reject
- sdrop

Fonctionnalités III

Éléments d'une règle

- Une action
- Un protocole
- (Adresse source, port source) et (adresse destination, port destination)
- Un opérateur indiquant la direction du flux (-> ou <>)

Exemple

alert tcp any any <> 192.168.1.0/24 any (content-list :"adults" ; msg : "Adults list access attempt" ; react : block ;)

action / protocole / adresse IP / port / opérateur

Fonctionnalités IV

Quelques champs utiles

- msg
- sid
- classtype
- priority
- content
- uricontent

Fonctionnalités V

Exemple de type personnalisé

```
ruletype redalert
{
    type alert
    output alert_syslog: LOG_AUTH LOG_ALERT
    output log_tcpdump: suspicious.log
}
```

Introduction

Suricata

- IDS jeune mais actif
- Soutenu par The Open Information Security Foundation (OISF)
- Open source

Fonctionnalités I

Fonctionnalités modernes

- Support natif de l'IPv6
- Multi-threadé
- Accélération matérielle native (GPU avec CUDA, PF_RING)
- IPS natif
- Paramétrage CPU
  - Affectation d'un thread à un CPU
  - Affectation d'une famille de threads à un ensemble de CPU
  - Prise en compte des interruptions matérielles
- Extraction et l'inspection de fichiers
- Analyse de handshake TLS

Fonctionnalités II

Modules d'entrée IDS

- PCAP
  - live, multi-interfaces
  - offline
- PF_RING
- AF_PACKET

Modules d'entrée IPS

- NFQueue
  - Windows
  - Linux : multi-queue
- ipfw : pare-feu avec états pour systèmes BSD

Fonctionnalités III

Modules de sorties

- fastlog
- unified log (Barnyard 1 & 2, format utilisé par Snort)
- HTTP log (log format Apache)
- Prelude

Fonctionnalités avancées I

libHTP

- Parseur orienté sécurité du protocole HTTP
- Suivi de flux
- Décodage des flux compressés avec GZip

Exemple d'utilisation de libHTP

```
alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS \
(
msg: "ET CHAT Facebook Chat (send message) " ; \
flow : established,to_server ; content : "POST" ; http_method ; \
...
)
```

Fonctionnalités avancées II

Flowbits

- Condition booléenne
- Positionnement d'un drapeau

Flowint

- Définition de compteur
- Opérations arithmétiques

Exemple d'utilisation de Flowint

```
alert tcp any any -> any any (msg: "Counting Usernames" ; \
content : "jonkman" ; flowint: usernamecount , + , 1 ; \
flowint: usernamecount , > , 5 ;)
```

Snorby I

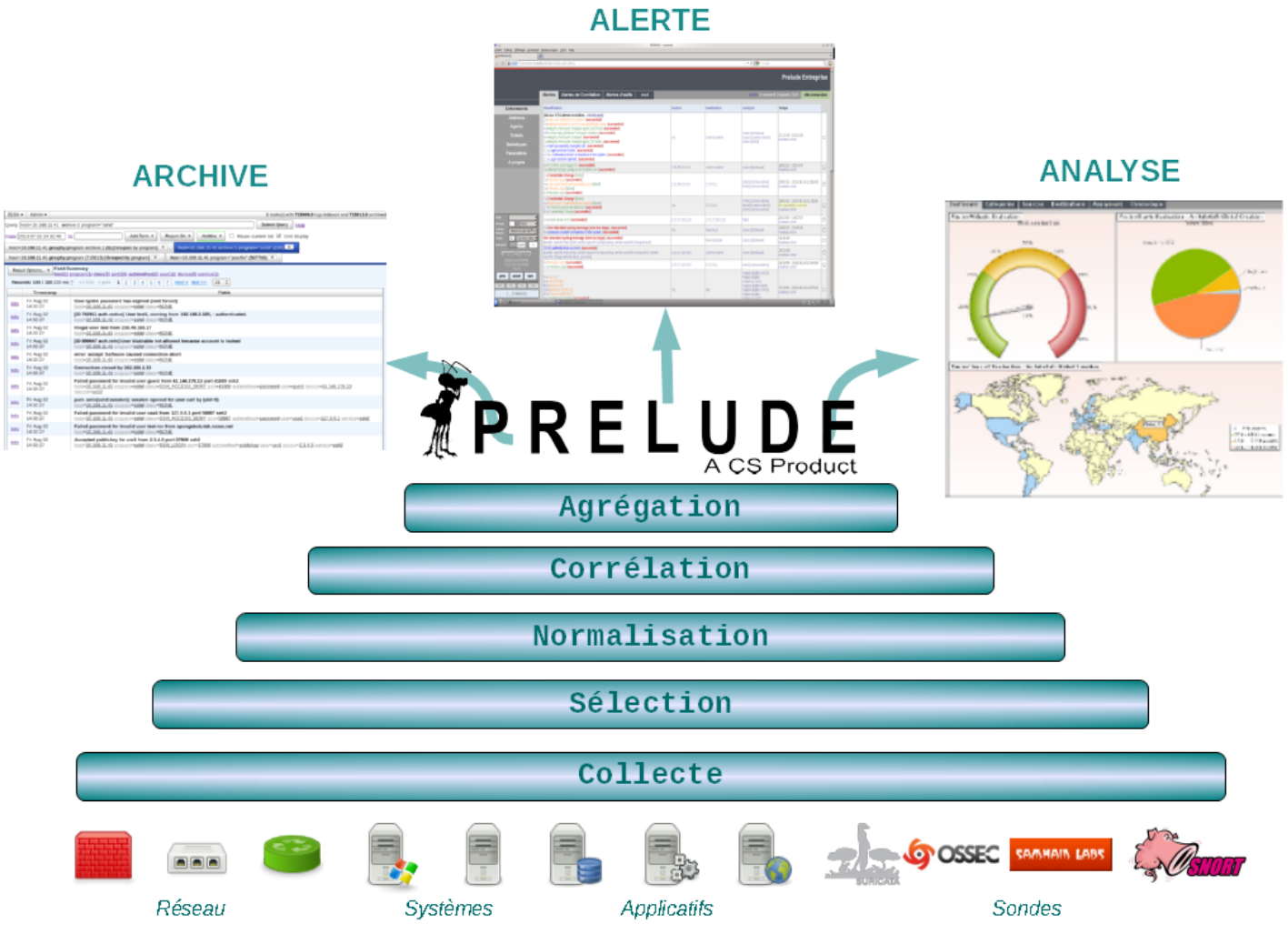
Fonctionnalités

- Interface web
- Monitoring
- Rapidité
- Simplicité
- Efficacité
- Temps réel, diagrammes, export, notifications ...
- 100% open source (Dustin Webber, Threat Track)

Snorby II


Snorby "All About Simplicity"
Welcome Demo | Settings | Log out
Dashboard
My Queue (8)
Events
Sensors
Search
Administration
Dashboard
More Options
LAST 24 TODAY YESTERDAY LAST WEEK THIS MONTH THIS QUARTER THIS YEAR
Updated: 03/19/12 12:05:52 AM
123
HIGH SEVERITY
123 / 200
46
MEDIUM SEVERITY
46 / 200
31
LOW SEVERITY
31 / 200
Sensors
Severities
Protocols
Signatures
Sources
Destinations
Event Count vs Time By Sensor
Snort
Suricata
Sagan
Event Count
Last 24 Hours
TOP 5 SENSOR
Snort 225,039
Suricata 200,241
Sagan 10,843
TOP 5 ACTIVE USERS
Dustin Webber 26
Demo 8
Champ Clark 0
LAST 5 UNIQUE EVENTS
[OPENSSH] Invalid or i... 1
[OPENSSH] Invalid or i... 2
[OPENSSH] Invalid or i... 2
[OPENSSH] Invalid or i... 1
[OPENSSH] Invalid or i... 2
ANALYST CLASSIFIED EVENTS
False Positive 374,990
Unauthorized Root Access 25,789
Reconnaissance 11,508
Attempted Unauthorized... 3,831
Policy Violation 1,481
Denial of Service Attack 560
Unauthorized User Access 393
Virus Infection 358
Snorby 2.5.0 - http://www.snorby.org © 2012 Dustin Willis Webber

Prelude I

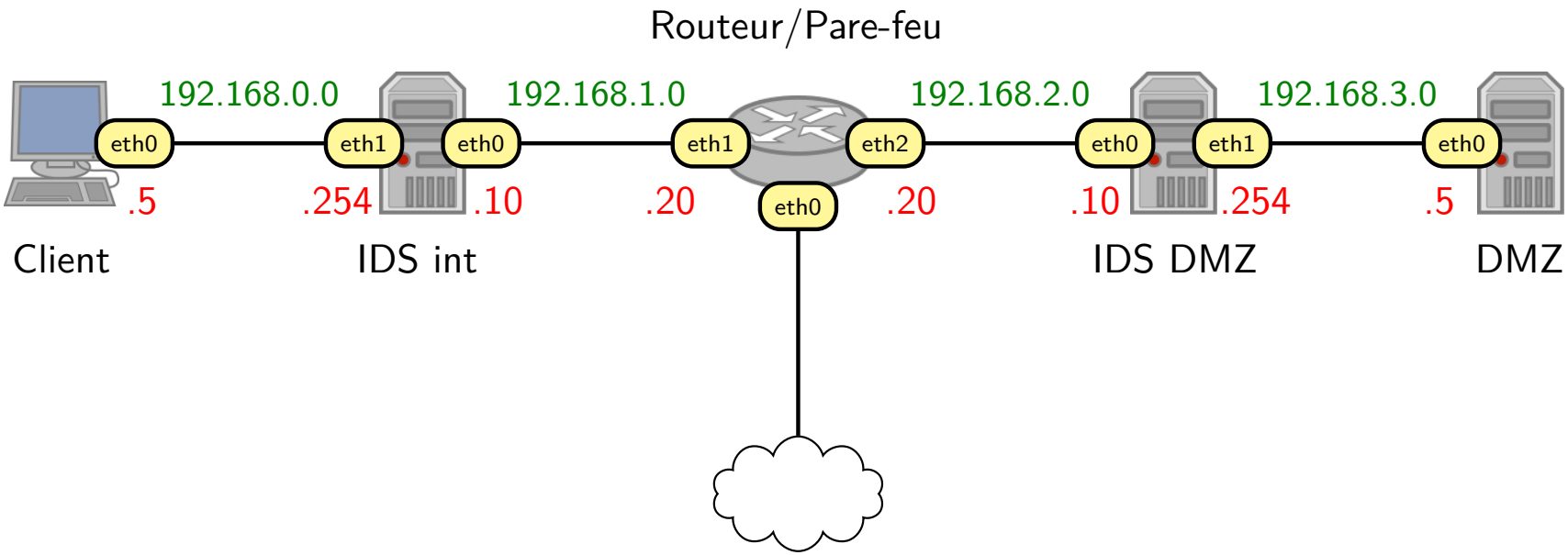

ALERTE
ARCHIVE
ANALYSE
PRELUDE
A CS Product
Agrégation
Corrélation
Normalisation
Sélection
Collecte
OSSEC
SAMHAIN LABS
OSHORT
Réseau
Systèmes
Applicatifs
Sondes

Prelude II

Actions post-normalisation

- Archiver
  - ↪ audit
  - ↪ juridique
- Analyser
  - ↪ comprendre l'attaque
- Alerter
  - ↪ corriger les failles

Réseau utilisé



Attaques & règles de filtrage I

Scan avec nmap

```
# nmap -sS 192.168.3.5
```

Règle Snort

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any ( \
msg:"DEMO-ATTACKS Scan NMAP"; dsize: 0; sid:7348;)
```

Attaques & règles de filtrage II

Injection SQL dans l'URL

```
# links "http://192.168.3.5/index.html?login=OR 1=1"
```

Règle Snort

```
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS ( \
msg:"DEMO-ATTACKS SQL injection"; \
uricontent:"OR 1=1"; sid:6969;)
```

Attaques & règles de filtrage III

Injection XSS dans une requête POST

```
POST /index.html HTTP/1.0
Content-Length: 31

<script>alert("toto")</script>
```

Règle Snort

```
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS ( \
msg:"DEMO-ATTACKS XSS attack"; content:"<script"; \
sid:7373;)
```

Attaques & règles de filtrage IV

Journalisation des erreurs 403

```
# links http://192.168.3.5/demo.html
```

Règle Snort

```
alert tcp $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET \
any (msg:"DEMO-ATTACKS 403 Forbidden"; \
content:"HTTP/1.1 403"; sid:73421;)
```

Attaques & règles de filtrage V

Fuite de /etc/passwd

```
# links http://192.168.3.5/../etc/passwd
```

Règle Snort

```
alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS ( \
msg:"DEMO-ATTACKS /etc/passwd"; \
uricontent:"/etc/passwd"; content:"/etc/passwd"; \
sid:8455;)
```

Conclusion

Récupérer le projet

`http://github.com/legrajul/projet_reseau`
↪ documents
↪ lab netkit de test

Des questions ?